Extreme Networks Education

Training Manual

[illegible]

EWC-200c

ExtremeWare CLI Switch Layer 2/Layer 3 Management and Configuration Training

STUDENT GUIDE

Revision 2.0
January 2002

For latest course offerings & schedules, visit our web site:

http://www.extremenetworks.com/apps/training/main.asp

© 2002 Extreme Networks, Inc. All rights reserved.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without permission from Extreme Networks, Inc.

Specifications and all other information regarding the products in this training manual are subject to change without notice. All information, statements, and recommendations in this manual are believed to be accurate. They are, however, presented without warranty of any kind, express or implied. The users of this manual must take full responsibility for their application of any products.

Extreme Networks, BlackDiamond, Ethernet Everywhere, Extreme Ethernet Everywhere, ExtremeWare, Summit, ServiceWatch and the color purple are registered trademarks of Extreme Networks, Inc. in certain jurisdictions. Alpine, Alpine 3804, Alpine 3808, BlackDiamond 6808, BlackDiamond 6816, Extreme Standby Router Protocol, ESRP, Summit1i, Summit5i, Summit7i, Summit24, Summit48, Summit48i, SummitGbX, SummitRPS, Epicenter, Extreme Velocity, the BlackDiamond logo, the Alpine logo, the Summit logo, the ExtremeWorks logo and the Extreme Networks logo are trademarks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. Extreme Turbodrive, the Extreme Turbodrive logo, ExtremeWorks, ExtremeWorks Professional Services and Go Purple are service marks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. All other registered trademarks, trademarks and service marks are property of their respective owners. Specifications are subject to change without notice.

EWC-200c – ExtremeWare CLI Switch Layer 2/Layer 3 Management & Configuration - Student Guide
Revision 2.0 – January 2002

Table of Contents

Chapter 1	Introduction and Orientation	7
Chapter 2	ExtremeWare Overview	37
Chapter 3	CLI Switch Management and Security	57
Chapter 4	Port Configuration	125
Chapter 5	Bridging Overview and Configuration	149
Chapter 6	VLAN and Port Configuration	175
Chapter 7	Spanning Tree Configuration	241
Chapter 8	IP Unicast Routing and Configuration	289
Chapter 9	RIP Configuration	333
Chapter 10	OSPF Overview and Configuration	371
Chapter 11	ESRP Overview and Configuration	449
Chapter 12	Introduction to QoS	505

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 1

Introduction & Orientation

Chapter Objectives

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

- **Introduction**
  - Instructor/Student Introductions
  - Facilities
  - Student Kit/Documentation
  - Administrative
- **Course Pre-requisites**
- **Course Objectives**
- **Agenda**
- **Summary**

Notes:

Introduction

Provide your name, company, job title and experience.

Students are encouraged to share their previous networking experience, as well as any Extreme Networks product exposure. This well help the instructor to level the class according to student skill sets.

© 2001 Extreme Networks,Inc. All rights reserved

Introduction

- **Instructor**
  - Name: Jon Black
  - Company:
  - Job Title:
  - Experience: jblack@sp.net

- **Students**
  - Name/Company
  - Job Title/Responsibility
  - Network Experience - Number of Years
  - Extreme Networks Product Exposure
  - Course Expectations

Notes:

Facilities

Familiarise yourself with the facilities, particularly where the restrooms are.

Breaks are at least 15 minutes each and lunch is about an hour. However, at the discretion of the instructor, the times may vary.

Provide the training site telephone number where messages can be sent. However, only urgent messages will be posted immediately for the attention of the student concerned.

Specify any special parking requirements when necessary.

© 2001 Extreme Networks,Inc. All rights reserved

Facilities

- **Restrooms**
- **Breaks**
  - AM Break
  - Lunch
  - PM Break
- **Telephones**
  - Messages
- **Parking**

Notes:

© 2001 Extreme Networks,Inc. All rights reserved

Student Kit

- Training Manual
- Extreme Networks Welcome Gift
- Pen and Marker
- Note Pad
- Name Tent

Notes:

Administrative

A class roster will be passed out by the instructor within the first hour of the class. Each student should check the information about them on the roster. When all information has been verified, the student should initial their names.

Ensure that your name is spelled exactly as you would want it to appear on the certificate at the completion of this course.

Students should turn off mobile phones. At the instructor's discretion, pagers/phones in vibrate mode are permitted. However, if you need to take a phone call, please leave the classroom in consideration of the other students.

Questions are encouraged any time.

Lectures are best done in the morning or early part of the afternoon. Lab exercises are designed to be performed after a major topic has been discussed or after a concept had been tackled.

A final written exam is to be given at the end of the course, prior to handing out the certificate of completion.

A student completing all the requirements for completion of the Extreme Networks Technical training will be handed an Extreme Networks Certified Training Certificate.

© 2001 Extreme Networks,Inc. All rights reserved

Administrative

- Class Roster/Sign-In Sheet
- Questions in Class
- Lecture
- Lab Exercises
- Course Challenge Exercise (TBD)
- Pagers and Mobile Phones
- Course Evaluation

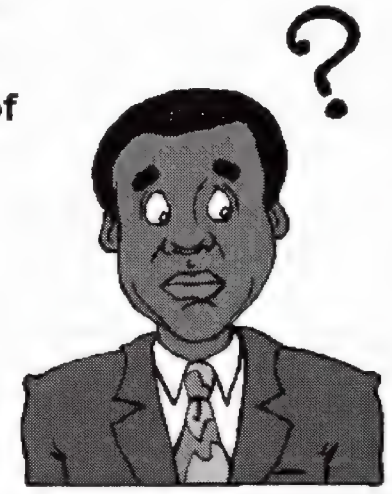
Notes:

Course Knowledge Pre-requisites

© 2001 Extreme Networks,Inc. All rights reserved

Course Knowledge Pre-requisites

- LAN Fundamentals
- TCP/IP, IP Addressing and Subnet Mask
- Switching, Bridging and Routing Concepts
- Familiarity with Extreme Networks Family of Switch Products & Architecture
- Web-based pre-course reading



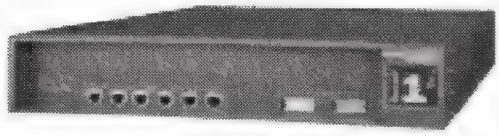
Notes:

EWC 5-day Course Objectives

© 2001 Extreme Networks,Inc. All rights reserved

EWC 5-day Course Objectives

- Describe Extreme Networks switch architecture and wire speed switching products.
- Prepare the Summit switch for deployment; navigate the command interface, view statistics, and effect configuration through a console connection, a telnet session, and a web browser.
- Describe 802.1q VLANs. Create and configure port-and-protocol sensitive and MAC based VLANs. Assign port and IP addresses to VLANs.
- Configure a switched network running Spanning Tree Protocol.
- Troubleshoot a basic layer 2 network.
- Describe basic theories of broadcast domains and IP forwarding and the differences between the OSI layer-2 and layer-3 in data forwarding.
- Construct a simple network using static routes and verify IP Unicast routing on the switch using the CLI commands.



Notes:

More Course Objectives

© 2001 Extreme Networks,Inc. All rights reserved

More Course Objectives

- Describe the benefits of dynamic routing, route loop resolution, and the features of distance-vector routing protocol.
- Configure and deploy a dynamically routed network using multiple Summit switches and the Routing Information Protocol (RIP).
- Describe the basic theories behind a link-state protocol, and link-state advertisements and the link-state database in OSPF.
- Configure and deploy a multi-router, multi-area OSPF network.
- Describe the deployment of redundant, stand-by VLANs in a routed environment and configure a fault-tolerant network using the Extreme Standby Router Protocol (ESRP)
- Describe and configure simple QoS parameters.
- Describe and configure simple Access Control List

Notes:

Day 1 -Agenda

© 2001 Extreme Networks,Inc. All rights reserved

Day 1 - Agenda

- **Chapter 1 - Introduction and Orientation**
- **Chapter 2 – ExtremeWare Features Overview**
- **Chapter 3 - CLI Switch Management and Security**
  - Lab1 – CLI Familiarization
  - Lab2 – More CLI - Download Image and Upload Configuration
  - Lab3 – ExtremeWare Vista Familiarization (optional)
  - Lab4 – BootROM Familiarization
- **LUNCH**
- **Chapter 4 – Ports Configuration**
  - Lab5 – Port and Load Sharing Configuration
- **Chapter 5 – Bridging Overview and Configuration**
  - Lab6 – FDB Configuration Familiarisation

Notes:

Day 2 -Agenda - VLANs

© 2001 Extreme Networks,Inc. All rights reserved

Day 2 – Agenda - VLANs

- **Chapter 6 – VLAN and Port Configuration**
  - Lab 7 – Port-Based VLAN Configuration I
  - Lab 8 – Port-Based VLAN Configuration II
  - Lab 9 – VLAN Configuration III with Tags
  - Lab 10- MAC-Based VLAN Configuration
  - Lab 11- vMAN Configuration Familiarisation

- **LUNCH**

- **Chapter 7 – Spanning Tree Configuration**
  - Lab12 – Spanning Tree Configuration

Notes:

Day 3 -Agenda

© 2001 Extreme Networks,Inc. All rights reserved

Day 3 – Agenda

- **Chapter 8 – IP Unicast Routing and Configuration**
  - Lab13 – IP Forwarding Configuration
- **Chapter 9 – RIP Routing Protocol**
  - Lab14 – RIP Configuration
- **LUNCH**
- **Chapter 10 – OSPF Overview and Configuration**
  - Lab15 – OSPF Configuration I
  - Lab16 – OSPF Configuration II

Notes:

Day 4 - Agenda - Routing with OSPF

© 2001 Extreme Networks,Inc. All rights reserved

Day 4 – Agenda – Routing with OSPF

- **Chapter 10 – OSPF Overview and Configuration cont..**
  - Lab17 – OSPF Configuration III
  - Lab18 – OSPF Configuration IV
- **LUNCH**
- **Chapter 11 – ESRP Overview and Configuration**
  - Lab19 - ESRP Configuration
- **Chapter 12 – QoS**

Notes:

Day 5 -Agenda

© 2001 Extreme Networks,Inc. All rights reserved

Day 5 - Agenda

- **Chapter 12 – QoS…cont**
  - Lab20 - QoS Configuration
  - L2 Network Challenge
  - L3 Network Challenge
- **LUNCH**
- **Course Wrap-Up**

Notes:

Summary

© 2001 Extreme Networks,Inc. All rights reserved

Summary

- **Introduction**
  - **Instructor/Student Introductions**
  - **Facilities**
  - **Student Kit/Documentation**
  - **Administrative**
- **Course Pre-requisites**
- **Course Objectives**
- **Agenda**

Notes:

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 2

ExtremeWare Overview

Chapter Objectives

The main theme of chapter two is to provide an overview of the Extreme Networks product family, including hardware, software, and the Extreme Networks switch architecture.

Upon completion of this chapter, you will be able to:

- Understand Extreme Networks Switch Architecture
- Define the ExtremeWare Software
- Describe ExtremeWare features and current release versions

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

Upon completion of this chapter, you will be able to:

- **Describe briefly the Extreme Networks Product family**
- **Understand Extreme Networks Switch Architecture**
- **Define the ExtremeWare Software**
- **Describe ExtremeWare Features and Current Release versions**

Notes:

Extreme Networks Switch Family

Extreme Networks stackable Summit switches, modular Alpine Ethernet service provisioning switches and modular BlackDiamond core switches meet evolving business requirements by delivering scalable speed, bandwidth, network size and quality of service to today's networks.

Within each Summit, Alpine and BlackDiamond is a non-blocking switch fabric that provides full wire-speed Layer 3 and Layer 2 performance all the time. The backplane capacity of Summit, Alpine and BlackDiamond is greater than the aggregation of all its ports, so data is not lost - even when the network load requires all ports to deliver full gigabit bandwidth.

All Extreme Networks switches come pre-installed with the ExtremeWare standards-based software suite. ExtremeWare combines industry-standard protocols to ensure interoperability with legacy switches and routers, plus Policy-Based Quality of Service (QoS) for bandwidth management and traffic prioritisation in today's networks.

The product range includes:

Desktop Switches

- Summit24e3
- Summit24e2
- Summit24
- Summit48

Data Centre

- Alpine 3808/3804/3802
- Summit1i
- Summit5i
- Summit7i
- Summit48i

Core Switches

- BlackDiamond 6816
- BlackDiamond 6808
- Alpine 3808/3804/3802

Application Switching

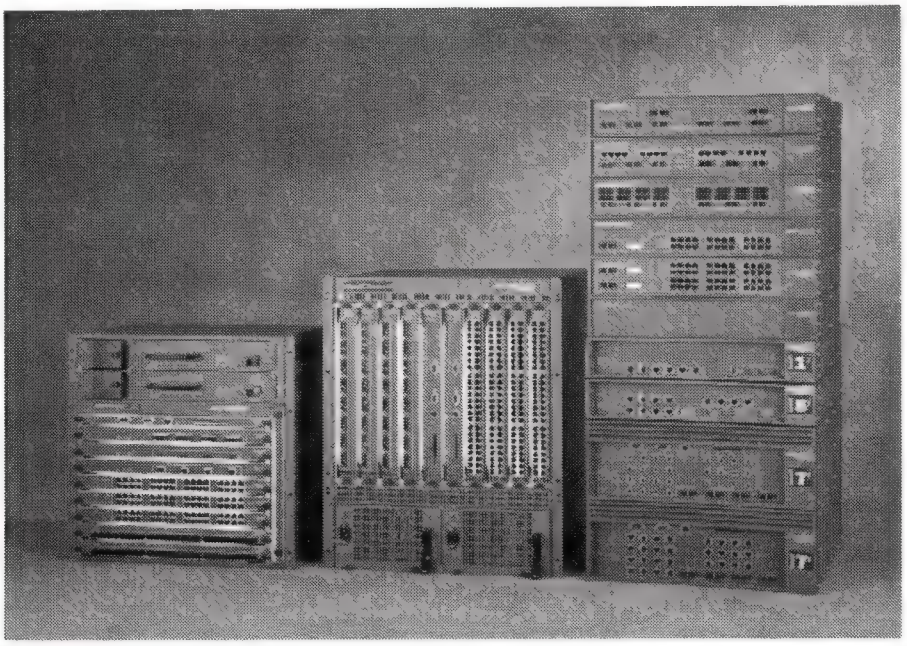
- SummitPx1

Software

- ExtremeWare (EW)
- EPICentre
- ExtremeWare ServiceWatch (ESW)

© 2001 Extreme Networks,Inc. All rights reserved

Extreme Networks Switch Family



ExtremeWare™

Notes:

Extreme Networks Switch Architecture

The Extreme Networks Switch Architecture is based on a single ASIC (Application Specific Integrated Circuit) chipset, comprised of several chips. Wire-speed forwarding is made possible through Extreme Networks proprietary ASIC design and implementation of core technologies.

Extreme Networks develop their own ASICs internally. It is the core of Extreme Networks products, and is entirely home grown, designed and manufactured. These chips are much more powerful than traditional methods used. The ASIC chipset can get deeper into gathering information, other than getting just MAC address (such as going into Layer 3 IP information etc.), than traditional software based routers.

The Summit architecture includes i-chipset and non-i-chipset ASICs. These have been optimised for wire-speed routing of IP traffic and Layer 2 switching of all other protocol traffic. The i-chipset represents the next generation of switches from Extreme Networks, which incorporate higher levels of integration and increased functionality at wire-speed. The i-chipset enables the development of switches with as much as four times the port density and performance.

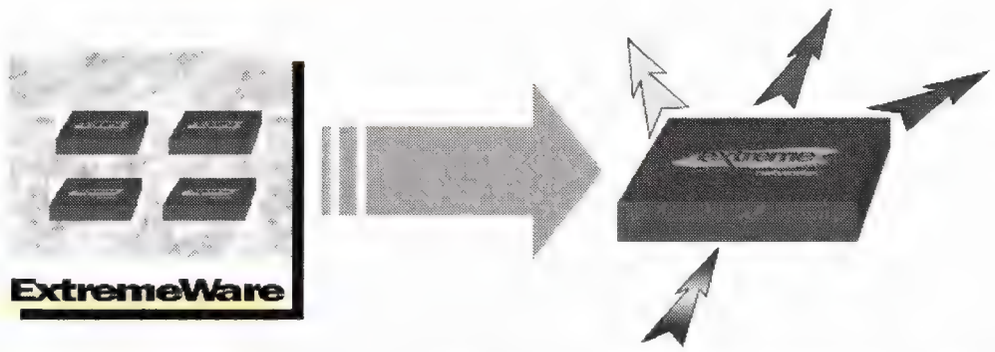
All products utilise Extreme Networks software product called "ExtremeWare". The power of ExtremeWare is the cross-functionality of the Command Line Interface (CLI), which makes information learned on any product directly transferable to any other because the syntax of the commands is the same.

i series - cost more

© 2001 Extreme Networks,Inc. All rights reserved

Extreme Networks Switch Architecture

- **Proprietary ASIC design & implementation of Core Technologies**



- **The switch fabric is comprised of a collection of ASIC chipsets**

CPU ← configuration are on CPU

Fabric — route : talk to "fabric" instead of CPU → increase the network speed (faster).

Notes:

reliability of connectivity - ASIC (積體)

Consistent Architecture

The unparalleled performance and consistent functionality across the entire family of Summit, Alpine and BlackDiamond switches are the result of the i-chipset and non-i chipset. With Extreme Networks switches, all processing that is required for forwarding packets at Layer 2 or Layer 3 is performed by these custom ASICs.

Full ASIC-based forwarding engines deliver more than 10-times higher throughput than routers that rely entirely on microprocessors. Like legacy routers, Extreme Networks switches use microprocessors to perform network management functions and to update route tables using standard protocols such as RIPv1, RIPv2, OSPF, DVMRP and PIM. However, processing route-table updates occur outside the data path and therefore do not affect forwarding performance.

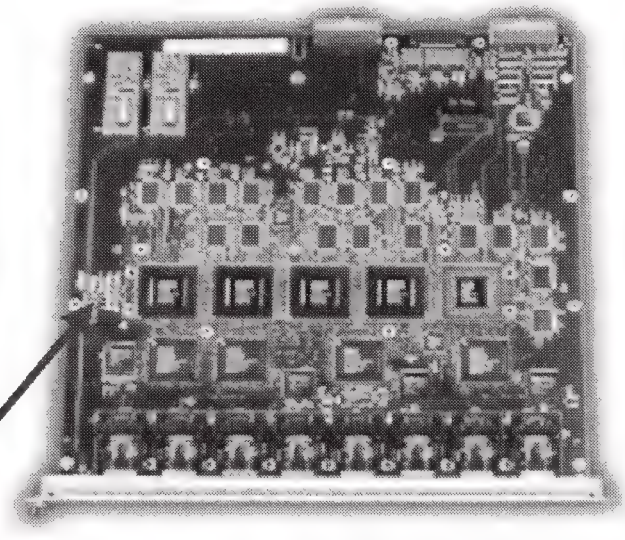
One unique addition to the i-chipset is that wire-speed IPX packet forwarding is also performed. This optimisation allows Summit, Alpine and BlackDiamond switches to take full advantage of high-performance custom silicon and a 64-byte-wide data path to perform wire-speed routing and switching with low latency.

Summit, Alpine and BlackDiamond switches also deliver wire-speed IP Routing (Layer 3 switching) as well as wire-speed Layer 2 switching. The wire-speed IP routing is performed by Extreme Networks custom ASICs, rather than by using software, this enables consistent wire-speed forwarding on all ports, all the time, simultaneously. Extreme Networks switches do not require hardware upgrades to achieve wire-speed performance and the switches do not require different software loads to optimise one function over another. This is the way true routing and switching was meant to be.

© 2001 Extreme Networks,Inc. All rights reserved

Consistent Architecture

- **Product Chipsets**
  - Non-i chipset
  - i chipset
    - Next Generation
  - Summit
    - i and non-i chipsets
  - BlackDiamond
    - i and non-i chipsets
  - Alpine
    - i-chipset only



Notes:

wire speed - no latency.

"i" Architecture

The i-chipset leverages the consistent architecture and feature set of the first-generation chipset, but with four times the density, twice the clock speed and half the power consumption per port.

In addition to the consistent architecture and feature set, the QoS Manager and Traffic Group Controller (TGC) have been integrated into the newer ASIC. Protocol Processing is increased with Dual Processors running 64 bit @ 166 MHz.

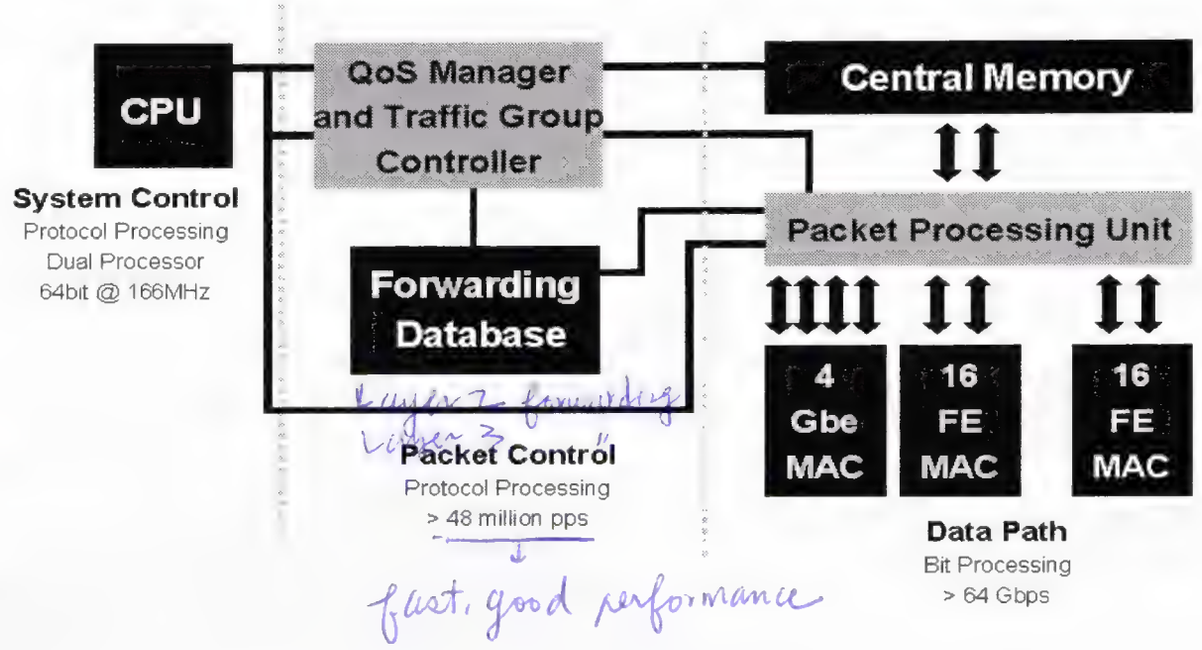
All Extreme Networks products that end with an "i", from the Summit stackables to BlackDiamond chassis blades, are based on the new i-chipset ASIC. i-chipset products require ExtremeWare version 6.1 or higher.

Non-Blocking Switch Fabric

The architecture of the Summit, Alpine and BlackDiamond switches have a non-blocking switch fabric that eliminates the performance penalties associated with slower legacy router environments. This means that the internal capacity of every Extreme Networks switch matches or exceeds the full-duplex bandwidth requirements of its ports. Operating in full-duplex mode on each port, Summit, Alpine and BlackDiamond switches process a full gigabit of data in each direction. The result is that our hardware architecture will never cause packet loss.

© 2001 Extreme Networks,Inc. All rights reserved

"i" Architecture



Layer 2 forwarding
Layer 3

fast, good performance

Notes:

Switch Fabric

Save in RAM Because CPU can't handle it

non-blocking switch Fabric

① in RAM

② fast

③ without storing anywhere

What is ExtremeWare?

ExtremeWare was developed to be the reliable, resilient operating system software that runs on all Extreme Networks i-chipset and non-i-chipset series switches. Common code offers some obvious advantages, starting with plug-and-play compatibility on Extreme Networks product lines. These products include – Summit (i and non-i-chipsets), Alpine (i) and BlackDiamond (i-and non-i chipset) switches.

Common code also means that consistent behaviour and stable performance can be taken for granted, right out of the box. And since this shared software runs on a shared switching architecture, customers are doubly protected against the sort of problems that can drag response time right down or even knock a web site out of commission.

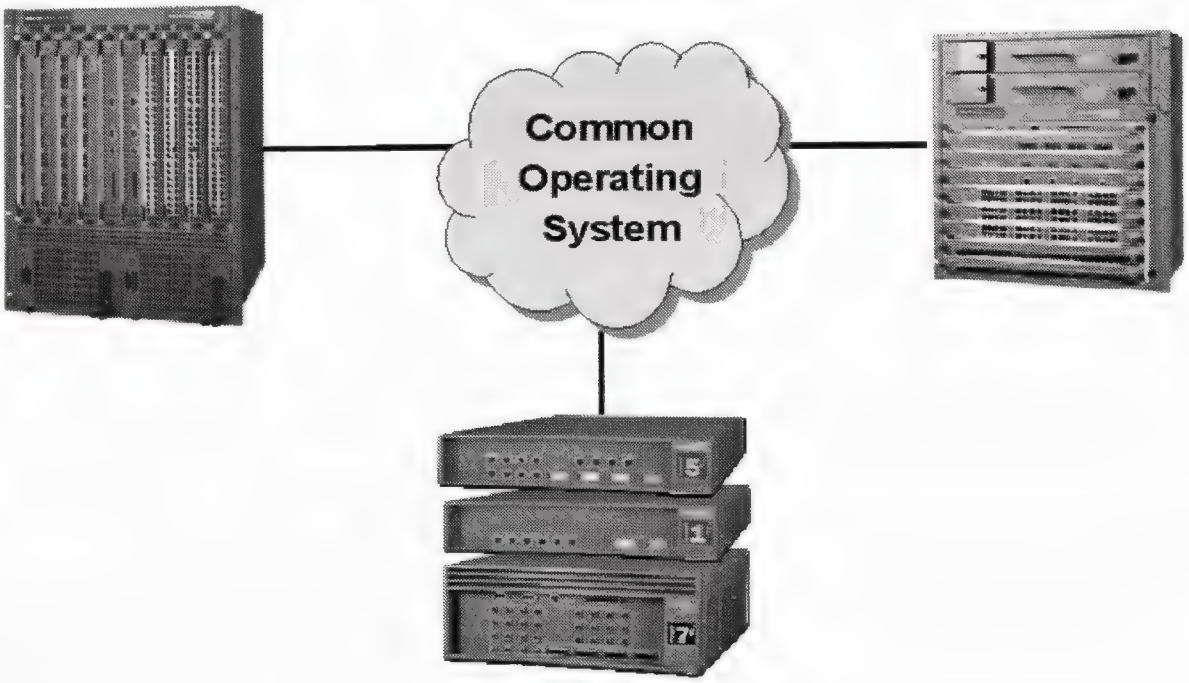
ExtremeWare delivers the uncompromising management, control and security needed on the largest networks, along with unsurpassed scalability. Additionally, standards-based multilayer switching and Policy-Based Quality of Service (QoS) give service providers and corporate networks the tools they need to make the most of their capacity.

ExtremeWare can set up and manage thousands of Virtual LANs (VLANs) for each switch. This gives service providers plenty of room to scale their infrastructure to meet customer demand while identifying and facilitating secure traffic across their networks. ExtremeWare also accommodates all commonly implemented VLAN types, ensuring maximum flexibility. These include VLANs based on protocol, port, and media access control (MAC) addresses, as well as 802.1Q tagging and generic VLAN registration protocol (GVRP).

For support purposes, Extreme Networks always recommend the most current release of ExtremeWare. If you are an Extreme Networks Assist customer, the latest release and release notes are available through the support login portion of the Tech Support web site at http://www.extremenetworks.com/

© 2001 Extreme Networks,Inc. All rights reserved

What is ExtremeWare?



Notes:

ExtremeWare Features

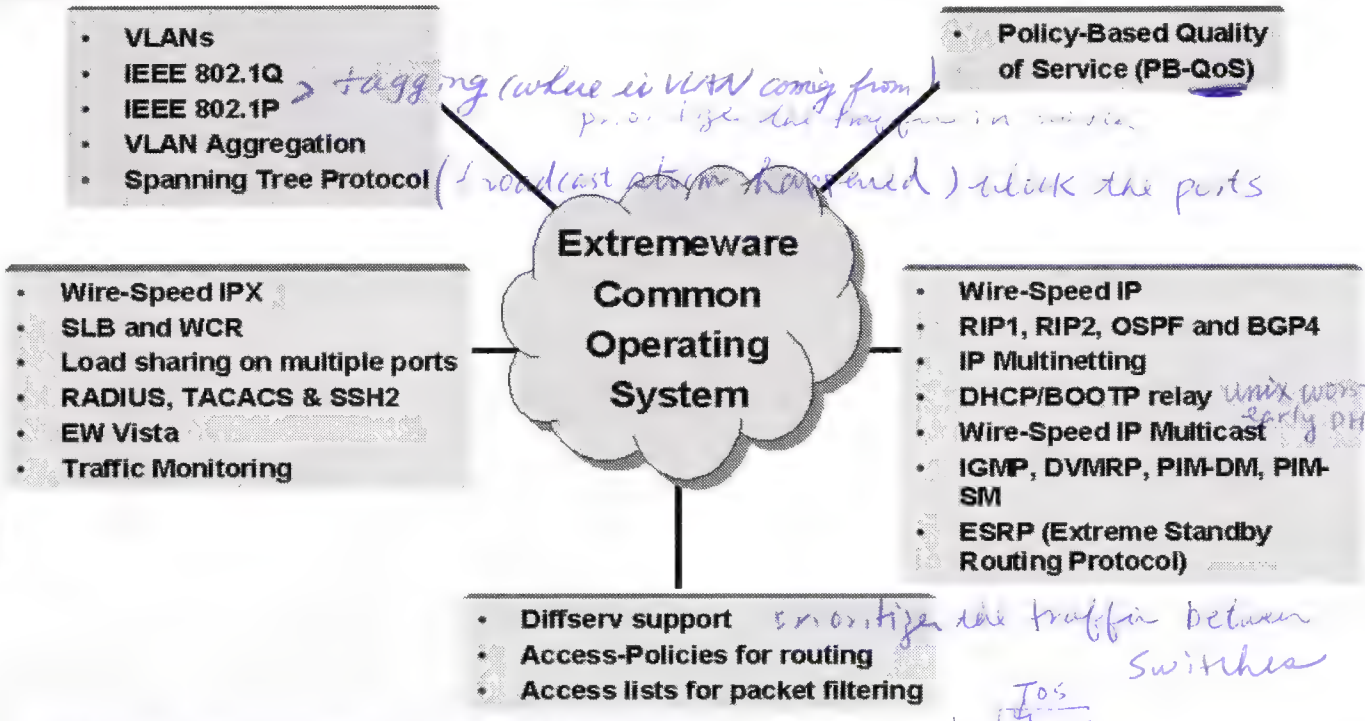
ExtremeWare is the full-featured software operating system that is designed to run on the BlackDiamond, Alpine, and Summit families of Gigabit Ethernet switches. The main features of ExtremeWare include the following:

- VLANs - including support for IEEE 802.1Q and IEEE 802.1p
- VLAN aggregation
- Spanning Tree Protocol (STP) (IEEE 802.1D) with multiple STP domains
- Policy-Based Quality of Service (PB-QoS)
- Wire-speed Internet Protocol (IP) routing
- IP Multinetting
- DHCP/BOOTP Relay
- Extreme Standby Router Protocol (ESRP)
- Routing Information Protocol (RIP) version 1 and RIP version 2
- Open Shortest Path First (OSPF) routing protocol
- Border Gateway Protocol (BGP) version 4
- Wire-speed IP multicast routing support
- Diffserv support
- Access-policy support for routing protocols
- Access list support for packet filtering
- IGMP snooping to control IP multicast traffic
- Distance Vector Multicast Routing Protocol (DVMRP)
- Protocol Independent Multicast-Dense Mode (PIM-DM)
- Protocol Independent Multicast-Sparse Mode (PIM-SM)
- Wire-speed IPX, IPX/RIP, and IPX/SAP support
- Server Load Balancing (SLB) support
- Load sharing on multiple ports, across all blades
- RADIUS client and per-command authentication support
- TACACS+ support
- Console command-line interface (CLI) connection
- Telnet CLI connection
- SSH2 connection
- ExtremeWare Vista Web-based management interface
- Simple Network Management Protocol (SNMP) support
- Remote Monitoring (RMON)
- Traffic mirroring for all ports, across all blades (BlackDiamond only)

For more information on BlackDiamond 6808 switch components, refer to the BlackDiamond 6800 Switch Hardware Installation Guide. For more information on Alpine 3800 switch components, refer to the Alpine 3800 Switch Hardware Installation Guide. For more information on Summit switch components, refer to the Summit Hardware Installation Guide.

© 2001 Extreme Networks,Inc. All rights reserved

ExtremeWare Features



tagging (where is VLAN coming from)

(broadcast storm happened) block the ports

unix workstation early DHCP

prioritize the traffic between switches

QoS

broadcast didn't go through routers.

R

Client

server

IP helper: help client to server By using relay.

VLAN aggregation:

parent

child

Notes:

QoS - garantee BW

(garantee get out of switch no garantee to the Dest.)

ATM - only can garantee BW

IP multinetting:

4 entries in routing table

1 entry in routing table

ExtremeWare Management Software

Using ExtremeWare, you can manage the switch locally using the CLI, or remotely by using Telnet.

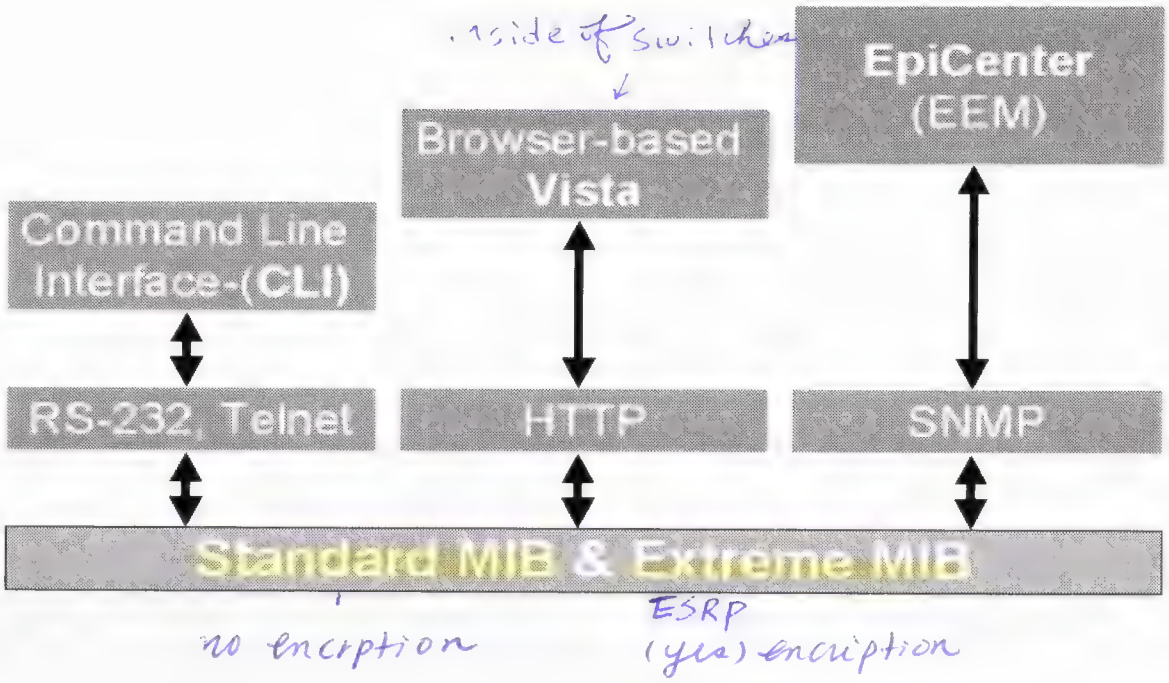
Access to the CLI is by connecting a terminal, (or workstation with terminal-emulation software) to the console port.

Access to the switch remotely is by using Telnet through one of the switch ports or through the dedicated 10/100 unshielded twisted pair (UTP) Ethernet management port (on switches that are equipped with one). Remote access includes the following:

- Telnet using the CLI interface
- SSH2 using the CLI interface
- ExtremeWare Vista Web access using a standard Web browser
- SNMP access using ExtremeWare Enterprise Manager or another SNMP manager

© 2001 Extreme Networks,Inc. All rights reserved

ExtremeWare Management Software



Notes:

Summary

Chapter two has provided an overview of the Extreme Networks Product family, the hardware and software architecture and ExtremeWare features. You should now be able to:

- Describe briefly the Extreme Networks Product family
- Understand Extreme Network Switch Architecture
- Define the ExtremeWare Software
- Describe ExtremeWare Features and Current Release versions

© 2001 Extreme Networks,Inc. All rights reserved

Summary

You should now be able to:

- **Describe briefly the Extreme Networks Product family**
- **Understand Extreme Networks Switch Architecture**
- **Define the ExtremeWare Software**
- **Describe ExtremeWare Features and Current Release versions**

Notes:

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 3

CLI Switch Management and Security

Chapter Objectives

Chapter three provides you with a structured examination of the Extreme Networks Switch Management & Security architecture. The Command Line Interface (CLI) is studied along with the syntax and basic commands.

Upon completion of this chapter, you will be able to:

- Describe ExtremeWare Management & Security
- Describe CLI structure and organisation
- Utilise CLI basic commands- create, config, enable and show
- Define ExtremeWare software, switch boot images and configuration files
- Utilise CLI commands - download, upload and use
- Define and configure the VLAN "Default"
- Learn additional management tools – SNMP, RMON, Logging and BootROM
- Successfully complete the lab exercises

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

Upon completion of this chapter, you will be able to:

- **Describe ExtremeWare Management & Security**
- **Describe CLI structure and organisation**
- **Utilise CLI Basic commands- create, config, enable and show**
- **Define ExtremeWare software, switch boot images and configuration files**
- **Utilise CLI commands - Download, Upload, & Use**
- **Define and configure the VLAN "Default"**
- **Describe additional management tools – SNMP, RMON, Logging and BootROM**
- **Successfully complete the lab exercises**

Notes:

CLI Organization

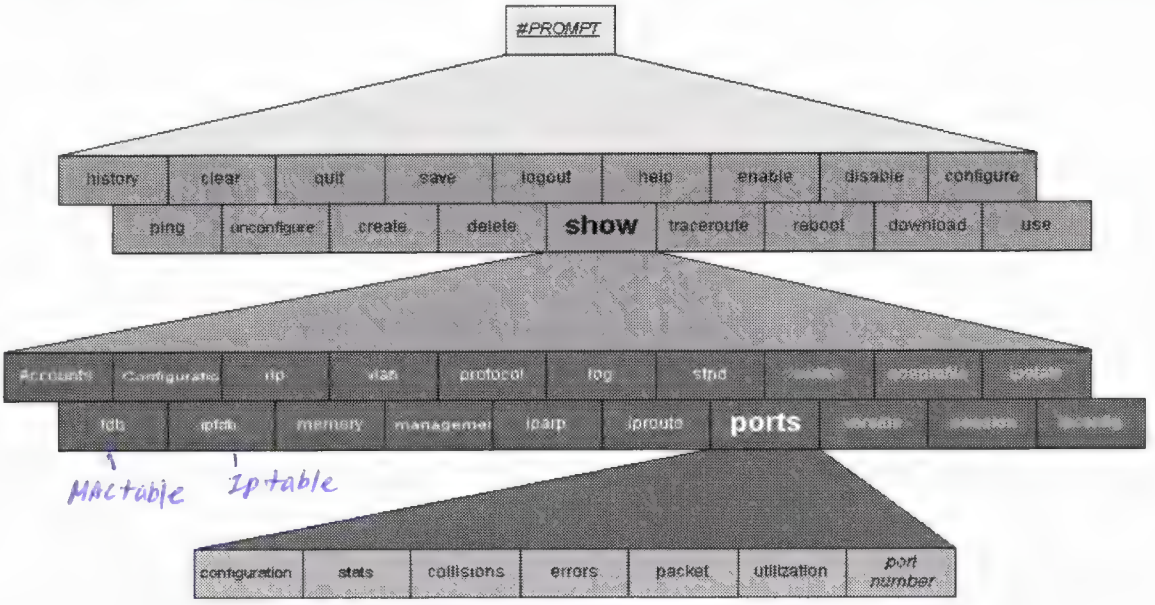
The Extreme Networks switch product range is accessible via the Command Line Interface (CLI) through either of two connections: via the Console Port or using a Telnet Session.

VISTA, the Web Based Management (WBM) application, is another way of managing the switch product range, although it must be remembered that not all configuration is possible using this interface.

CLI provides you with commands that are five to six layers deep, depending on the command. Most of the CLI commands are on the fly changes, in other words, it happens as you do it.

© 2001 Extreme Networks,Inc. All rights reserved

CLI Organization



Notes:

Syntax Helper

If you are unsure of the complete syntax for a particular command, enter as much of the command as possible. The syntax helper provides a list of options for the remainder of the command.

If you enter a partial command, pressing the [Tab] key displays any additional options, then repeats the command on a new line and places the cursor at the end of this new command line for completion. The use of the Tab key is invaluable. This goes all the way up to the root entry.

When entering a command at the prompt, ensure that you have the appropriate privilege level. Most configuration commands require you to have the administrator privilege level.

© 2001 Extreme Networks,Inc. All rights reserved

Syntax Helper

First-tier command: Using the **command completion** key displays all of the second-tier options

Previous command is echoed, Second and Third-tier commands are added to syntax string

Completed command syntax

```
Summit4:3 # show <tab>
Next possible completions:
        access-profile access-list access-list-fdb access-
         list-monitor accounts banner bgp configuration debug-
         trace dlcs dns-client dot1p dvmrp edp esrp
         fdb flow-redirect gvrp igmp iparp
         ipconfig ipfdb ipmc iproute ipstats
         ipxconfig ipxfdb ipxrip ipxroute ipxsap
         ipxservice ipxstats log mac-vlan management
         memory mirroring ospf pim ports protocol qosprofile
         radius radius-accounting rip route-map session slb
         slot sntp-client stpd switch tacacs tacacs-accounting
         tech-support udp-profile version vlan <udp forwarding
         profile> <access list> <access profile> <vlan name>
         <spanning tree name> <protocol name> <QOS profile>
         <flow redirect> <route map>

Summit4:3 # show port <tab>
Next possible completions:
    collisions configuration info packet qosmonitor
    rxerrors stats txerrors utilization <port number>

Summit4:3 # show ports configuration <tab>
Next possible completions:
        <cr>
Summit4:3 # show ports configuration
```

Notes:

Unique Name Identifiers

Unique and user-friendly names for VLANs, (and Spanning Tree Domains etc.), is made possible with the Unique Name Identifier function.

Naming a Virtual LAN (VLAN) or naming a Spanning Tree Domain (STPD) is unique. The switch knows, for example, that if you configure a VLAN with the name of purple, then purple is a VLAN as far as it is concerned and once configured, you only need to specify purple in any further commands.

The switch allocates some words for system use, these are reserved words and should be avoided for name identifiers (or their name truncations). An example of this reserved word usage might be:

Summit1i: # create vlan tim – creates a VLAN with the unique name of "tim"

Summit1i: # sh tim - results in the system time being displayed, and not the VLAN "tim"

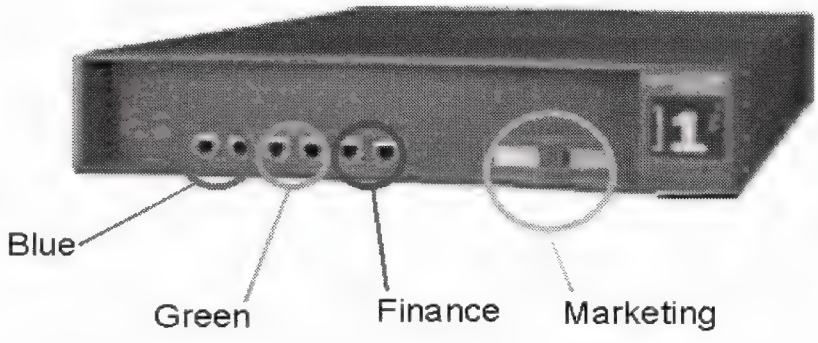
Also, name identifiers cannot be truncated like reserved words, for example:

Summit1i: # sh po conf - shows the switches port configuration

Summit1i: # conf def – which is the truncated name for "configure default", is not permitted

© 2001 Extreme Networks,Inc. All rights reserved

Unique Name Identifiers



- **Names are used as reference keys within the command set.**
- **Unique Name identifiers are used for naming VLANs, Spanning Tree protocol domains, etc.**

Notes: Don't use "red" "tim"

Abbreviated Syntax

Abbreviated syntax is the shortest, most unambiguous allowable abbreviation of a command, parameter, or value. This can be as short as the first letter of the command, but by convention is typically the first three letters. As already mentioned, please remember that name identifiers cannot be truncated like reserved words. Avoid misspelled words as the parser will not be able to recognise these.

Here is an example, using truncation, where you can reduce the command string by typing the following:

Summit1i: # co default a p 1-9 t n

The full command string is actually:

Summit1i: # configure default add ports 1-9 tag nobroadcast)
When listing the ports within a CLI command, you have the choice to:

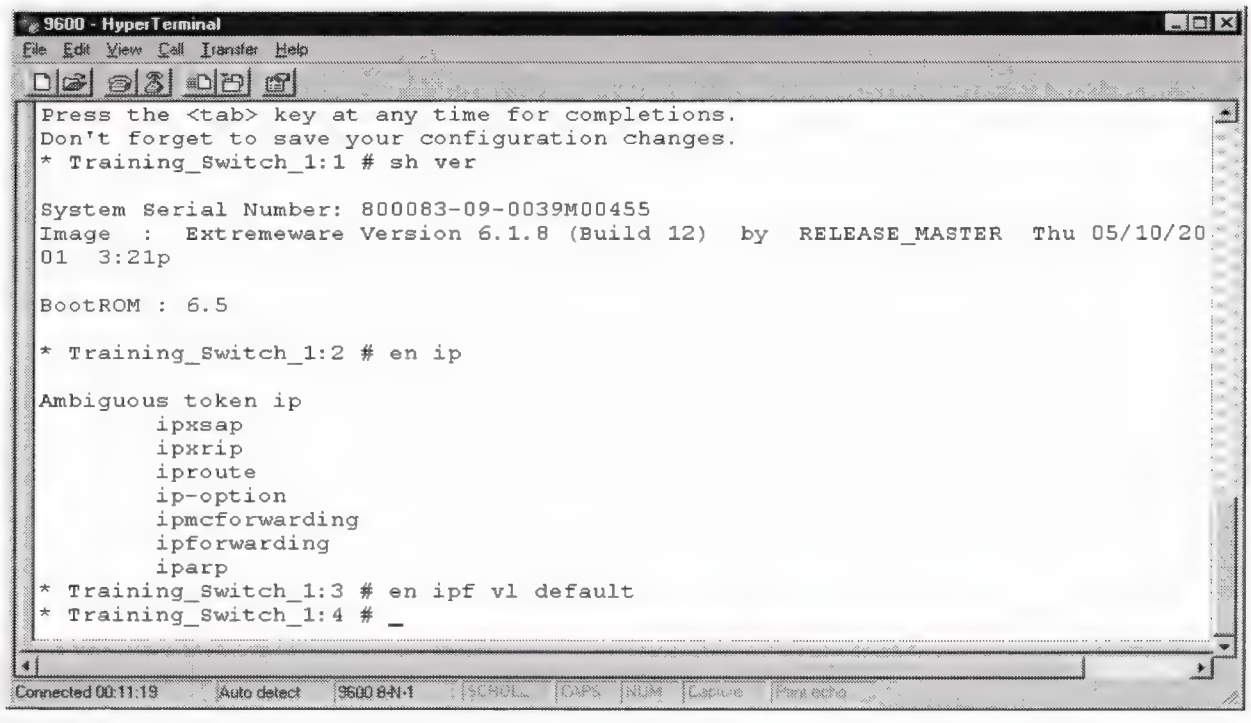
- List the ports separated by commas
- Range them, i.e. ports 1-9
- Name them all

Command History
The Extreme Networks switch "remembers" the last 49 commands entered and stores them in the command history buffer. The contents of this buffer can be displayed by entering the history command.

You can scroll through the command history buffer with the <Up> and <Down> arrow keys. Using these keys will echo the next or previous command in the buffer and place the cursor at the end of the command string.

© 2001 Extreme Networks,Inc. All rights reserved

Abbreviated Syntax



Notes:

CLI Access

The console can be used for direct local management, and the port settings are as follows:

- Baud rate - 9600
- Data bits - 8
- Stop bit - 1
- Parity - None
- Flow Control - XON/XOFF

The PC/Terminal connected to the switch's console port must be configured with the same settings. The CLI console port connection utilises physical switches to terminal connection using a serial cross cable (a.k.a. Null modem) with DB9 female connectors.

Connect one end of a serial cable to the console port on the switch. Note that the BlackDiamond, Alpine and Summit7i have the console port on the front of the switch, with all other Summits, it is on the rear of the switch. Note that the lower 9-pin serial port labeled as "modem" on the BlackDiamond MSM module does not allow any connectivity to the device at this time.

Connect the other end of the serial cable to the COM port of a terminal or PC running terminal emulation. Refer to the documentation supplied with the terminal equipment for the proper procedures in configuring the port settings.

Any workstation with a Telnet facility should be able to communicate with the switch over a TCP/IP network:

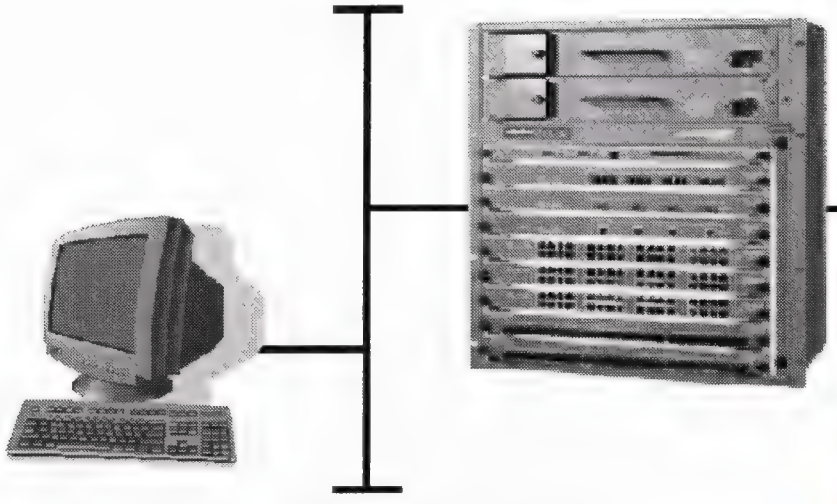
- Up to eight active Telnet sessions can access the switch concurrently
- The Telnet connection will time out after twenty minutes of inactivity
- If a connection to a Telnet session is lost inadvertently, the switch terminates the session within two hours
- Nested Telnet is also supported – but be careful

Before you can start a Telnet session, you must set up the IP parameters.

Some Extreme Networks switch models provide a dedicated 10/100 UTP management port. This port provides dedicated remote access to the switch using TCP/IP. Management via this port can be Telnet using the CLI interface, ExtremeWare Vista Web access, or SNMP access using ExtremeWare EpiCentre or another SNMP management application. The management port is a DTE port, and is not capable of supporting switching or routing functions. The TCP/IP configuration for the management port is done using the same syntax as is used for VLAN configuration. The VLAN mgmt comes pre-configured with only the 10/100 UTP management port as a member.

© 2001 Extreme Networks,Inc. All rights reserved

CLI Access



- Console Port Connection
- DB9
- 9600, 8, N, 1, X

Use cross-over cable

- Telnet Connection
- Up to 8 Sessions
- Needs IP to be configured up

Notes:

Switch Log-In

The Summit supports the following two levels of management (or CLI access privileges), these are:

- User
- Administrator

The Extreme Networks switch range can have a total of sixteen management accounts. You can use the default accounts names (admin and user), or you can create new accounts with different names and passwords.

The Extreme Networks Reference Guides specify that passwords must have a minimum of four characters and can have a maximum of twelve characters. However, names and passwords can also be entered that are between one and thirty-one characters. User names and passwords are case sensitive.

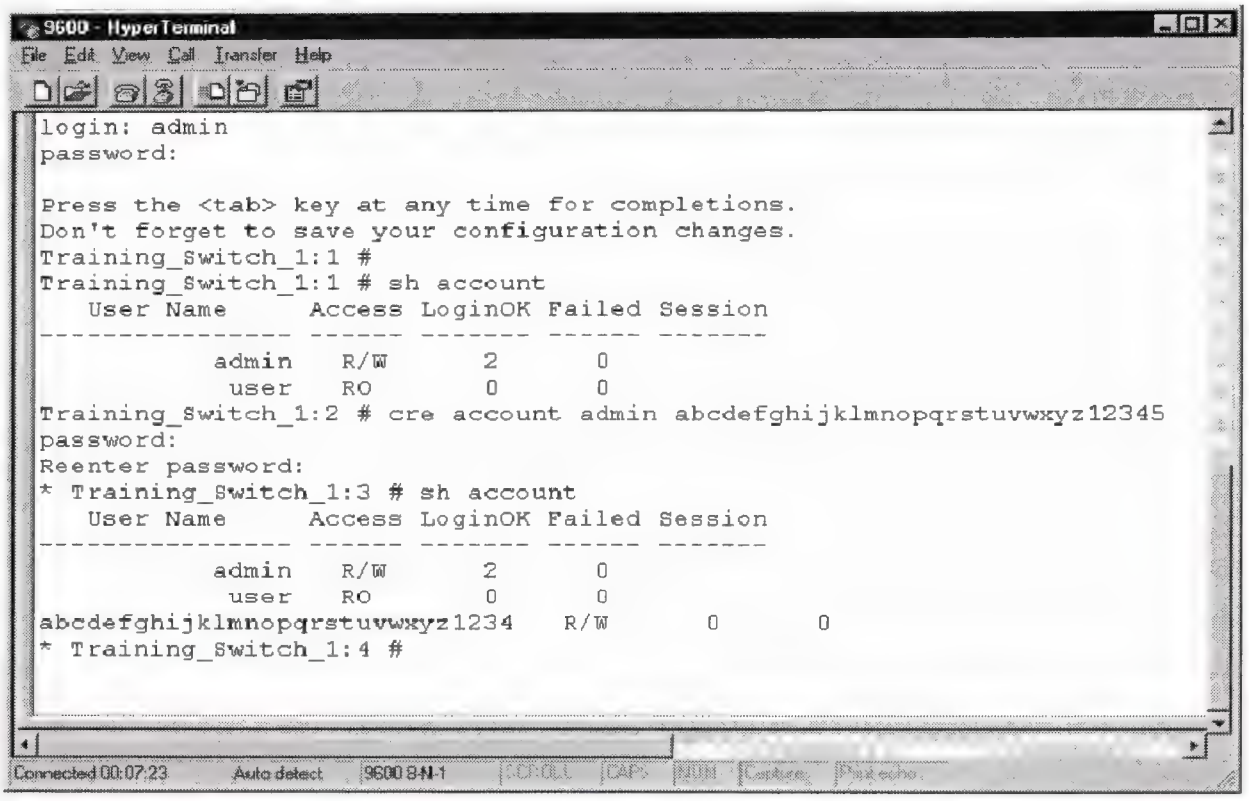
You can create two admin accounts, and they are identical in their power.

If you change, and then forget, the password for your only remaining Administrator Account on the switch, the password can ONLY be recovered in one of the following three ways:

- Provide dial-up, modem access to the switch console port and contact Extreme Networks Technical Support to provide a remote reset of the password
- Contact your Extreme Networks Systems Engineer to provide an on-site reset of the Administrator password
- RMA the switch to Extreme Networks in Santa Clara, California, where the password can be recovered and returned at your cost

© 2001 Extreme Networks,Inc. All rights reserved

Switch Log-In



Notes:

Switch Management Accounts

User Level Account
A user level account has viewing access to all manageable parameters, with the exception of the following:

- Showing the switch configuration
- Showing switch management details
- User account database
- SNMP community strings

A user-level account can use the ping command to test if a device is reachable, and change the password assigned to the account name. If you have logged on with user capabilities, the command-line prompt will end with a (>) sign.

Administrator Level Account
An administrator level account has read and write access to all manageable parameters. An administrator can perform the following functions:

- view and change all switch parameters
- add and delete accounts, and
- change the password associated with any account name
- disconnect a management session that has been established by way of a Telnet connection. If this happens, the user logged on by way of the Telnet connection is notified that the session has been terminated

If you have logged on with administrator capabilities, the command-line prompt will end with a (#) sign.

CLI Command - create account
create account [admin | user] <name> {encrypted} {<password>}
Creates a user account. Only users with admin level authority can create new accounts.

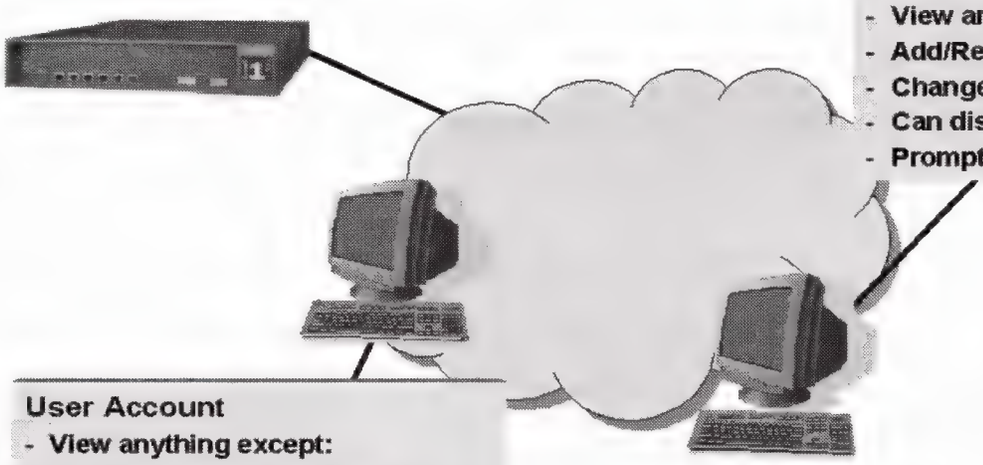
(The encrypted option should only be used by the switch, as it is a system option for switch to TFTP server uploads and downloads and not for users. If the encrypted option is used while creating a new account through the CLI, the switch will assume that the username and password are in its encrypted form and not in clear text. A login for this account with the clear text name and password will not be possible).

CLI Command - show account
The admin level "show account" command displays the following:

- account names
- access level
- number of successful and failed login attempts, and the number of active sessions in the user database

© 2001 Extreme Networks,Inc. All rights reserved

Switch Management Accounts



Administration Account
- View and change anything
- Add/Remove users
- Change user passwords
- Can disconnect Telnet sessions
- Prompt type: Summit48i #

User Account
- View anything except:
  - Show switch configuration
  - Show switch management
  - User Accounts
  - SNMP community strings
- Use PING
- Change Password
- Prompt type: Summit1i >

Notes:

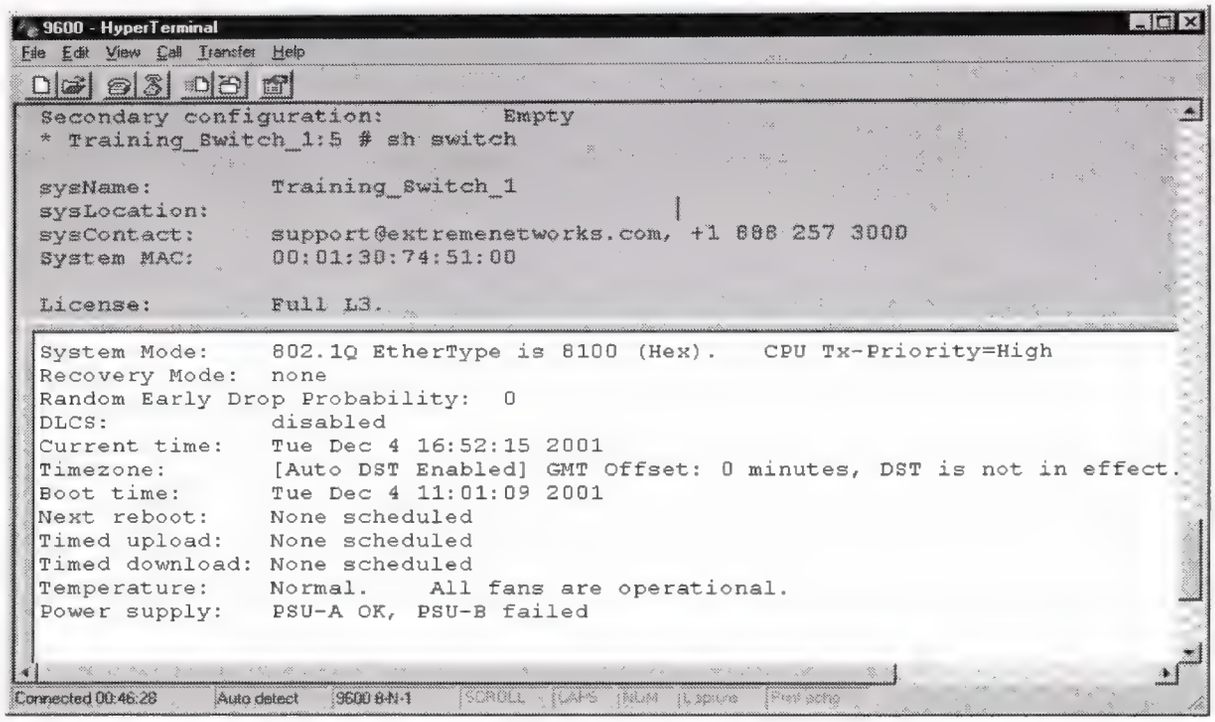
Show Switch Display - 1

The command "show switch" displays the current switch information, including:

- System name, system location, system contact
- MAC address
- Current date and time, and system boot time
- Operating environment (temperature, fans, and power supply status)
- NVRAM image (primary/secondary image, version)
- NVRAM configuration (primary/secondary configuration, date, time, size)
- Scheduled reboot information
- 802.1Q ethertype
- Power supply and fan status

© 2001 Extreme Networks,Inc. All rights reserved

Show Switch Display - 1



Notes:

Show Switch Display - 2

This is the continuation of the “show switch” display from the previous slide.

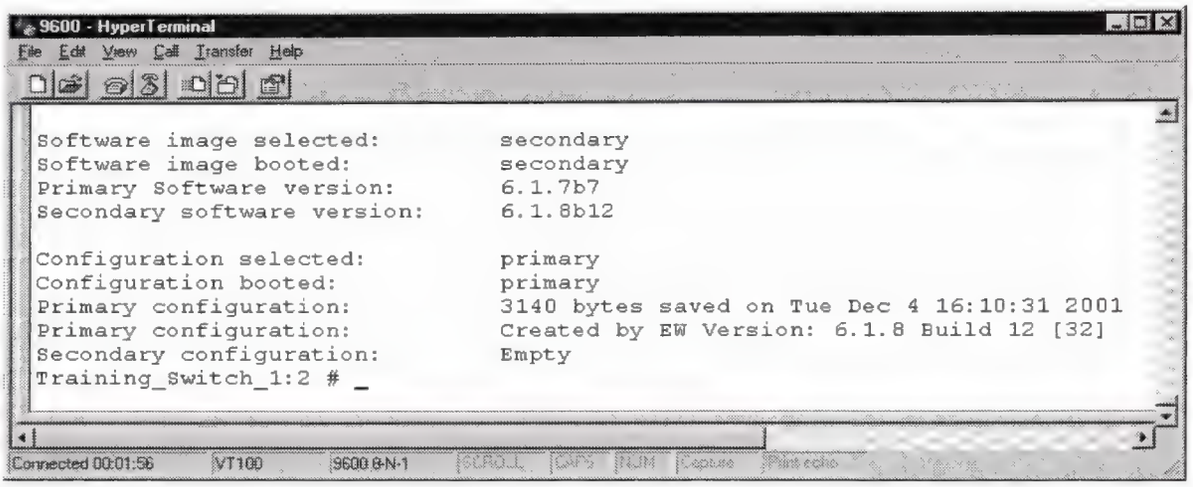
Note the current configuration booted from. In the current display, you can determine the software image file that the switch booted from and the configuration file it used to boot.

The software image selected may not necessarily be the software image file that the switch booted from, and the configuration file selected may not necessarily be the configuration file the switch has currently booted from.

In this example, the software image selected and booted is taken from the secondary location. The configuration selected and configuration booted is taken from the primary location.

© 2001 Extreme Networks,Inc. All rights reserved

Show Switch Display - 2


9600 - HyperTerminal
File Edit View Call Transfer Help
Software image selected: secondary
Software image booted: secondary
Primary Software version: 6.1.7b7
Secondary software version: 6.1.8b12
Configuration selected: primary
Configuration booted: primary
Primary configuration: 3140 bytes saved on Tue Dec 4 16:10:31 2001
Primary configuration: Created by EW Version: 6.1.8 Build 12 [32]
Secondary configuration: Empty
Training_Switch_1:2 # _
Connected 00:01:56
VT100
9600 8-N-1

Notes:

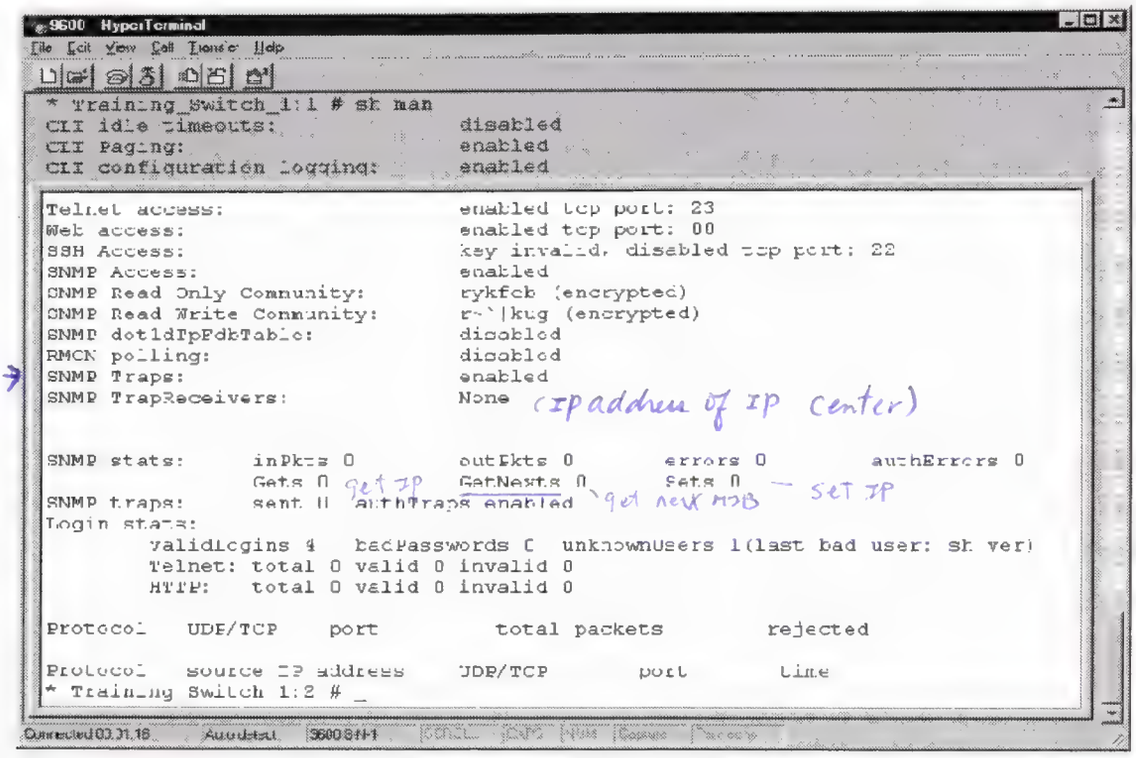
CLI Command - Show Management

The CLI command "show management" displays the network management configuration, statistics and SNMP settings configured on the switch. The command displays network management configuration and statistics, including:

- Enable/disable states for Telnet, SNMP, and Web access
- SNMP community strings
- Authorised SNMP station list
- SNMP trap receiver list
- RMON polling configuration
- Login statistics

© 2001 Extreme Networks,Inc. All rights reserved

CLI Command - Show Management


9600 HyperTerminal
File Edit View Call Transfer Help
* Training_Switch_1:1 # sh man
CLI idle timeouts: disabled
CLI Paging: enabled
CLI configuration logging: enabled
Telnet access: enabled tcp port: 23
Web access: enabled tcp port: 80
SSH Access: key invalid, disabled tcp port: 22
SNMP Access: enabled
SNMP Read Only Community: rykfcb (encrypted)
SNMP Read Write Community: r~`|kug (encrypted)
SNMP dot1dIpRdbTable: disabled
RMON polling: disabled
SNMP Traps: enabled
SNMP TrapReceivers: None (ipaddress of IP center)
SNMP stats: inPkts 0 outPkts 0 errors 0 authErrors 0
Gets 0 GetNexts 0 Sets 0
SNMP traps: sent 0 authTraps enabled
Login stats:
validLogins 4 badPasswords 0 unknownUsers 1(last bad user: sh ver)
Telnet: total 0 valid 0 invalid 0
HTTP: total 0 valid 0 invalid 0
Protocol UDP/TCP port total packets rejected
Protocol source IP address UDP/TCP port time
* Training_Switch_1:2 #
get IP
get next MIB
set IP
Connected 03:31:16
Auto detect
9600 8-N-1

Notes:

Trap - switch sends something I didn't ask for

ExtremeWare Software Versions

ExtremeWare is the full-featured software operating system that is designed to run on the BlackDiamond and Summit families of Gigabit Ethernet switches. The next few slides will discuss the latest ExtremeWare software release, differentiate between the software image files and that of the configuration files and present more CLI management commands.

The current release being shipped on newly manufactured switches is:

- Non-i switch products EW release 4.1.19
- Summit24, Summit48, Black Diamond 6808 with MSM32s

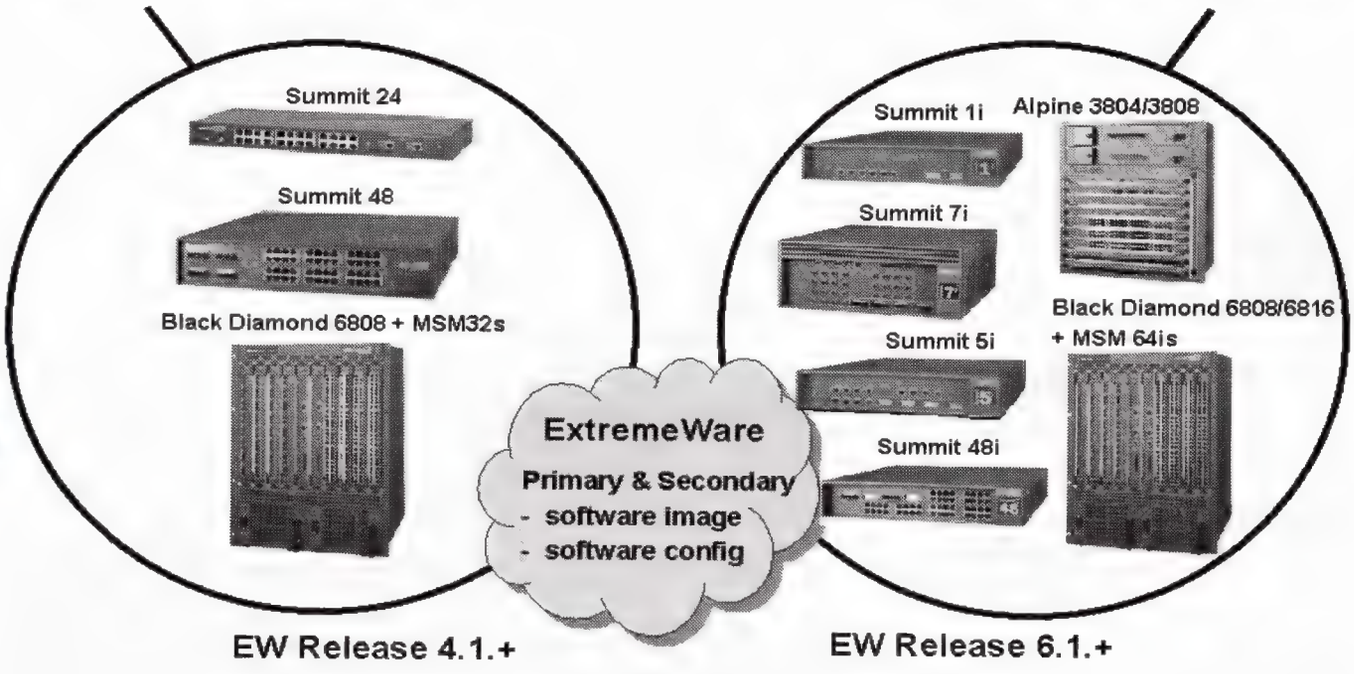
- i-based switch products – EW release 6.1.9
- Summit7i, 5i, 1i and 48i, Alpine 3804/3808, BlackDiamond 6808/6816 with MSM64is

Every switch loads a user-selected software operating system image file on boot.

In addition to loading a software operating system image, the switch also loads a software configuration file that contains customised sets of parameters, selected by the administrator, to run on a specific switch in th network.

© 2001 Extreme Networks,Inc. All rights reserved

ExtremeWare Software Versions



Notes:

Switch Software Image Files

Every Extreme Networks switch loads a user-selected software operating system image on boot. The image file contains executable code in a compressed format. An example of a Software image is EW Version v6.1.9b11 (build 11). The latest version of ExtremeWare is pre-installed on each switch released by Quality Control at the factory.

The switches can store two software operating system images; a primary and a secondary image. When downloading a new image, you must select which image space (primary or secondary) you want the new image to be placed into.

The primary and secondary software images are stored in Flash RAM. You may find it useful to use both primary and secondary image files, especially when upgrading software. If something goes wrong with an upgrade, you have a fallback image to boot from.

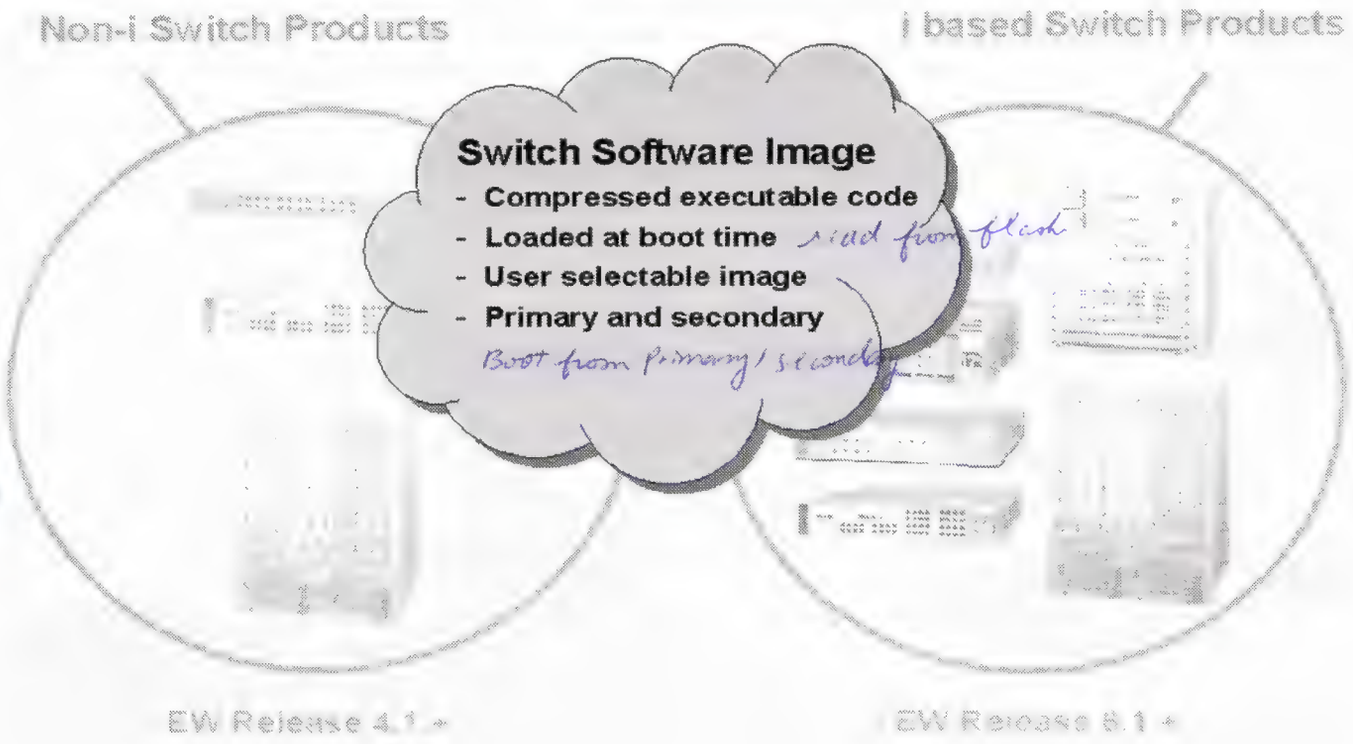
These containers, although called primary and secondary, are just place holders.

The standard way to load a software image is by using TFTP. However, in case of a corruption of the image file it is possible to load an image through the console port with an X-modem. This option is available throug the BootROM menu.

low speed (9600 Kbps)

© 2001 Extreme Networks,Inc. All rights reserved

Switch Software Image Files



Notes:

Switch Software Configuration Files

The software configuration is the customised set of parameters that the administrator has selected to run on the individual switch. If you make configuration changes, the new settings are stored in run-time memory.

- Settings stored in run-time memory are not retained by the switch when it reboots

To retain settings, and have them loaded when the switch reboots, you should save the configuration to nonvolatile storage by issuing one of these two CLI save commands:

- save primary
- save secondary

You can only TFTP the active configuration, and there are two configurations stored on the switch:

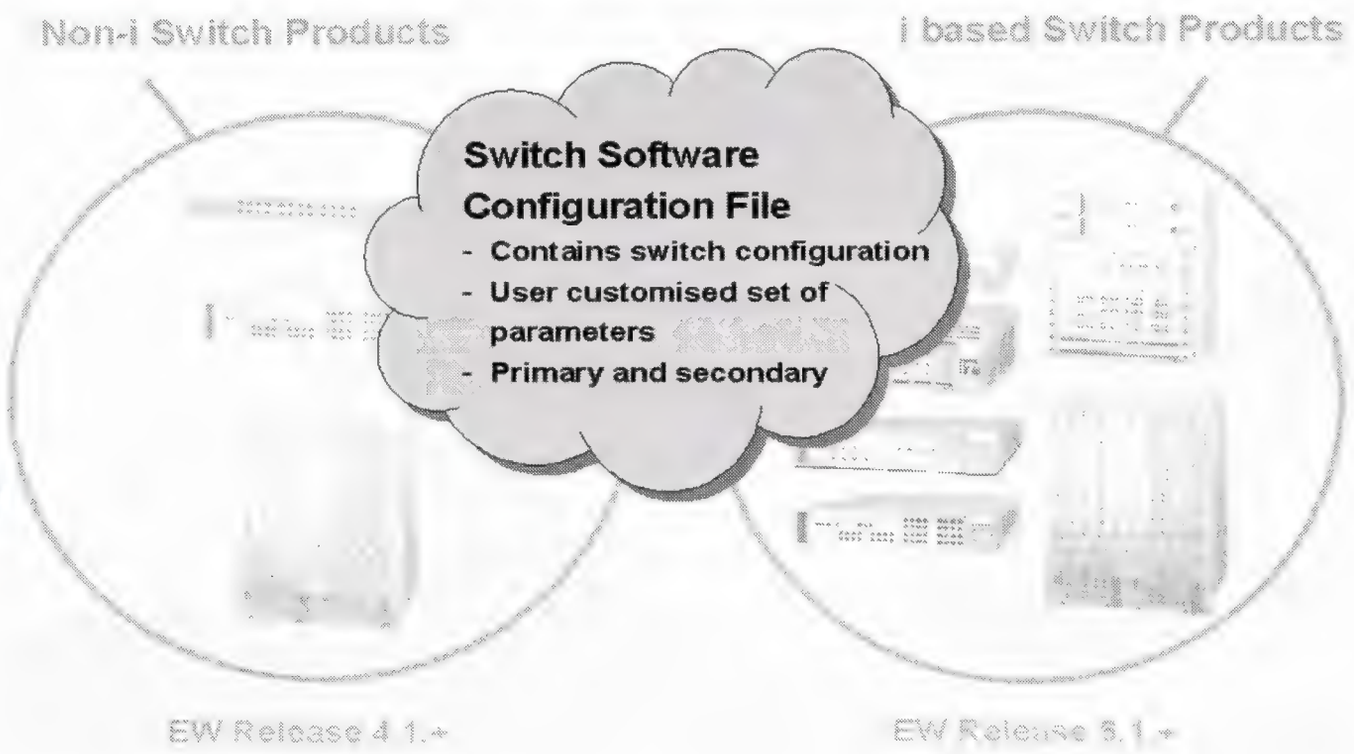
- These have no co-relationship to the primary or secondary image files
- The primary image can be running the secondary configuration and vice-versa

Note that the configuration files are not backwards compatible with the software image files. You should not run a configuration file created with, for example, v6.1.8b12 with software v6.1.7b9.

Software v6.1.9b11 and up will not allow a reboot if there is a mismatch between the image and the configuration file.

© 2001 Extreme Networks,Inc. All rights reserved

Switch Software Configuration Files



Notes:

Show Switch Display

An example display is shown on the slide as a result of entering the CLI command: show switch.

From the display example, note which software image is selected, and booted from.

In this case, what will be the software version booted from? _____

What other CLI command will verify the software version? _____

The configuration selected is that of primary and the switch configuration it used on boot is primary.

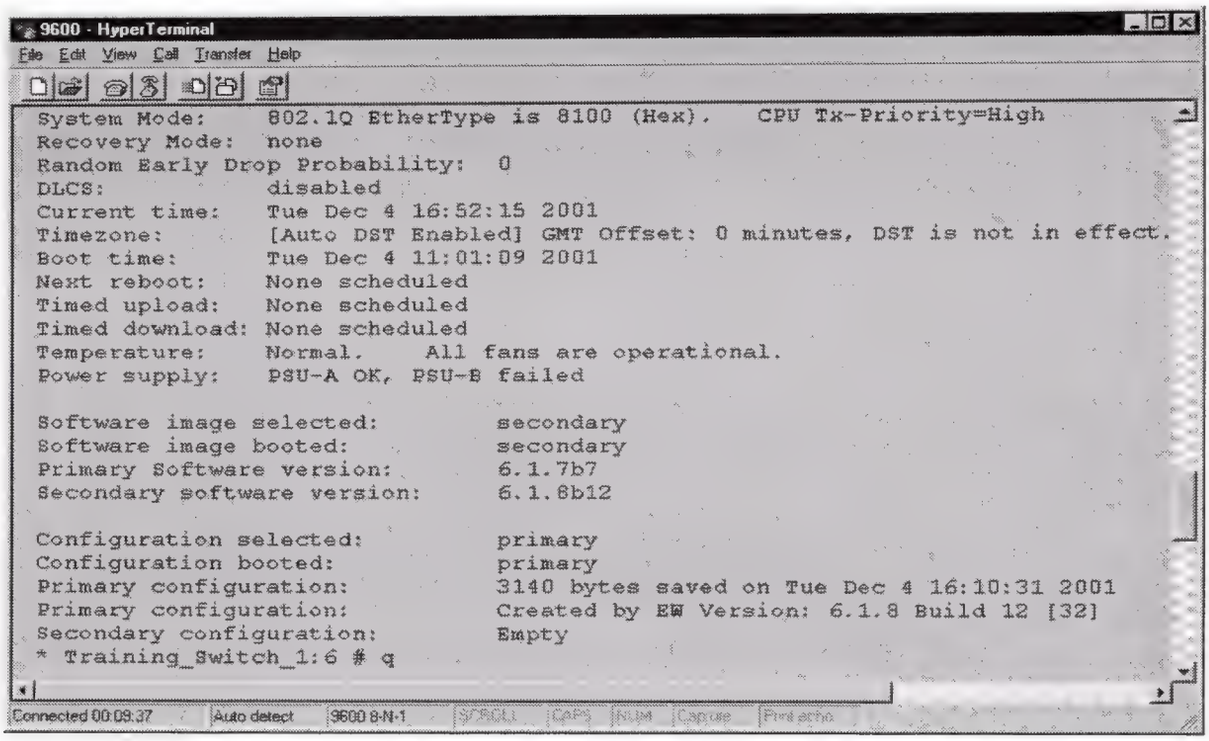
Is there a secondary configuration? _____. Is it different from the primary?
How do you know this?_____

Examine the command prompt after executing the "show switch", note the "*" preceding the prompt.

What does the "*" indicate? _____

© 2001 Extreme Networks,Inc. All rights reserved

Show Switch Display


9600 - HyperTerminal
File Edit View Call Transfer Help
System Mode: 802.1Q EtherType is 8100 (Hex). CPU Tx-Priority=High
Recovery Mode: none
Random Early Drop Probability: 0
DLCS: disabled
Current time: Tue Dec 4 16:52:15 2001
Timezone: [Auto DST Enabled] GMT Offset: 0 minutes, DST is not in effect.
Boot time: Tue Dec 4 11:01:09 2001
Next reboot: None scheduled
Timed upload: None scheduled
Timed download: None scheduled
Temperature: Normal. All fans are operational.
Power supply: PSU-A OK, PSU-B failed
Software image selected: secondary
Software image booted: secondary
Primary Software version: 6.1.7b7
Secondary software version: 6.1.8b12
Configuration selected: primary
Configuration booted: primary
Primary configuration: 3140 bytes saved on Tue Dec 4 16:10:31 2001
Primary configuration: Created by EW Version: 6.1.8 Build 12 [32]
Secondary configuration: Empty
* Training_Switch_1:6 # q
Connected 00:09:37
Auto detect
9600 8-N-1

Notes:

Downloading a New Image

The image is upgraded by using a download procedure from either a Trivial File Transfer Protocol (TFTP) server on the network or a PC connected to the serial port using the XMODEM protocol. The serial download can only be done from the BootROM menu. This should only be used if a recovery of the switch is needed.

Downloading a new image involves the following steps after IP connectivity has been properly set up:

- Load image onto a TFTP server
- Verify IP connectivity between switch and TFTP server
- Download image to switch
- Select which image to use on next reboot
- Reboot the switch

Note that 90% of the time, changes in the configuration of the switches does not require a reboot. A few of those that do include this download image procedure.

CLI Command – Download Image
download image <host name/ip><filename> {primary | secondary}
Downloads a new software image from a TFTP server over the network to one of the two storage containers, primary or secondary.
The download image command parameters are:

- Hostname/IP - ipaddress is the ipaddress of the TFTP server

  - Hostname is the hostname of the TFTP server

Note that the DNS client needs to be configured to use this option (configure dns-client).

- filename - is the filename of the new image

  - for example v618b12.xtr

- primary - indicates the primary image

- secondary - indicates the secondary image

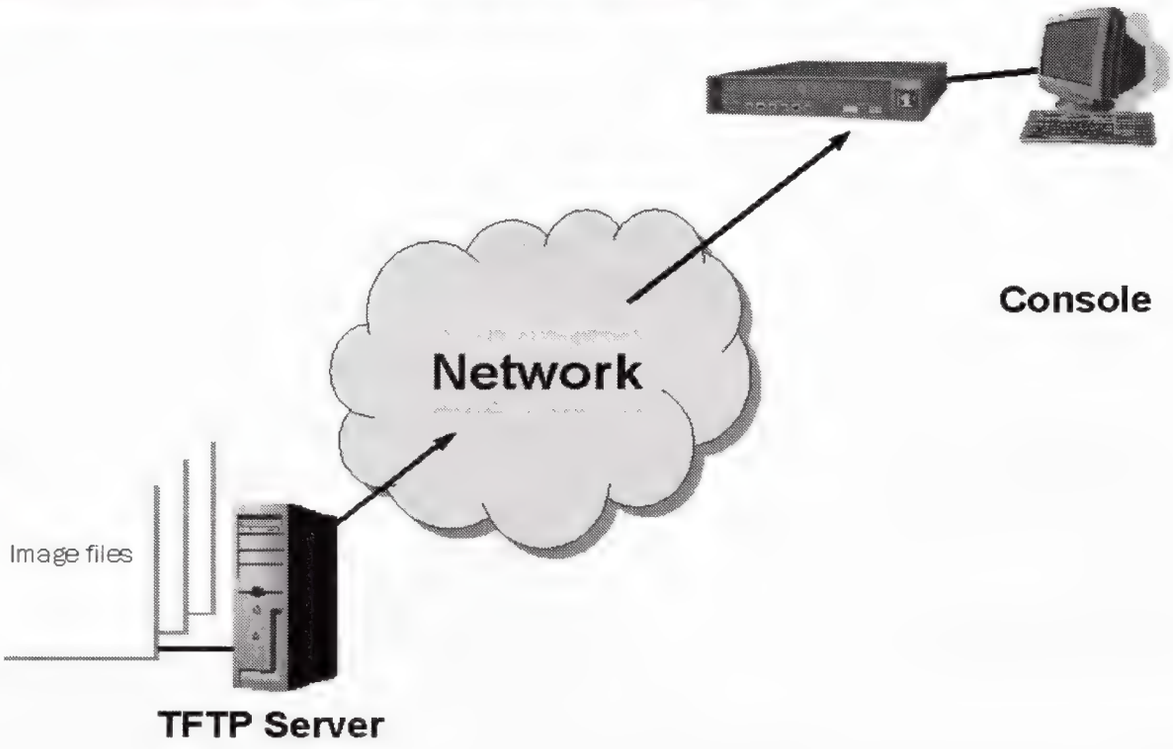
If no parameters are specified, the image is saved to the one selected for the next reboot.

CLI Command – Use Image
use image [primary | secondary]
Allows you to select which image the switch will load on the next reboot, for example, after a successful download image.

CAUTION: Make sure that your software image is compatible with the BootROM Master Release Version, i.e. BootROM Rel 1.9 for non-I chipset switches and Rel. 6.5 for the i-chipset switches. Note that software v6.1.9b11 requires BootROM v7.2.

© 2001 Extreme Networks,Inc. All rights reserved

Downloading a New Image



Notes:

read "release note"

Reasons to Upload Configuration

You can upload the current configuration to a TFTP server on your network. You can only upload the active configuration. The uploaded ASCII file retains the CLI format. This will allow you to do the following:

- Modify the configuration using a text editor, and later download a copy of the file to the same switch, or to one or more different switches
- Send a copy of the configuration file to the Extreme Networks Technical Support department for problem-solving purposes
- Automatically upload the configuration file every day, so that the TFTP server can archive the configuration on a daily basis. Because the filename is not changed, the configured file stored in the TFTP server is overwritten every day

CLI Command – Upload Config
upload config [cancel | <host name/ip> <filename>] {every <hour> <minute>}
Uploads the current runtime configuration to the specified TFTP server. If every <time> is specified, the switch automatically saves the configuration to the server once per day, at the specified time. To cancel automatic upload, use the cancel option. If no options are specified, the current configuration is uploaded immediately.

NOTE: Configuration files are plain text ASCII, and you can edit the configuration files with a plain text editor (don't use Word or Wordpad).

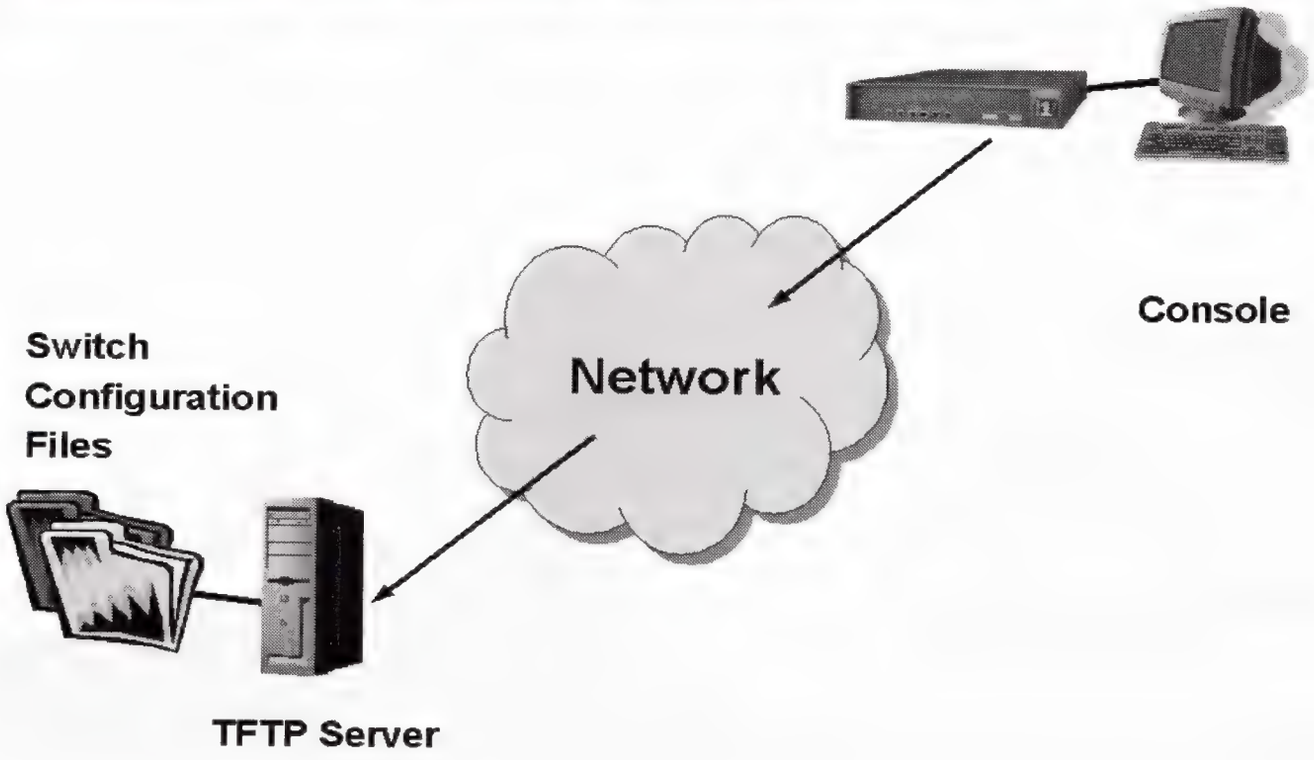
CLI Command – Download Config
download config [cancel | every <hour><minute> | <hostname/ip>] <filename> {incremental}
Downloads a previously saved ASCII configuration file from a specific TFTP server. After the ASCII configuration file is downloaded using TFTP, you are prompted to reboot the switch. The downloaded configuration file is stored in an area of switch memory, (not primary or secondary configuration containers) and is not retained if the switch has a power failure. When the switch is rebooted, it treats the downloaded configuration file as a script of CLI commands. After the script is executed, you should save the configuration to the primary or secondary configuration area, in order to retain it through a power cycle. If you are connected to the switch through the serial port, you are reminded that it is necessary to save the configuration to preserve it.

NOTE: You must reboot the switch if you made changes to the following default settings:
enable/disable web access (Default setting is enabled)
configure dot1Q ethertype <hex number>

Boot Rom - nobody kick out the cable
have to send back to extreme if
something happened in the middle

© 2001 Extreme Networks,Inc. All rights reserved

Reasons To Upload Configuration



Notes:

Saving the Configuration

CLI Command - Save
save {configuration} {primary | secondary}
Saves the configuration to the location selected, either primary or secondary. Remember to save your configuration every time you make changes to it.

Regardless of which download option is used, configurations are downloaded into switch runtime memory only. The configuration is saved only when you do the save command. If the configuration currently running in the switch does not match the configuration that the switch used when it originally booted, an (*) appears before the command line prompt when using the CLI.

NOTE: If the switch is rebooted while in the middle of a configuration save, the switch boots to factory default settings. The configuration that is not in the process of being saved is unaffected.

NOTE: You can only save the active configuration, not what is in primary or secondary. If you do a save <cr> the switch will query you to answer yes or no with this question:
à Do you want to save to the <selected container> configuration database?

CLI Command – Use Configuration
use configuration [primary | secondary]
Configures the switch to use a particular configuration on the next reboot. Options include the primary configuration area, or the secondary configuration area.

NOTE: Executing the USE CONFIG command does not make the configuration the active configuration. This just selects which configuration is going to be used after the next reboot.

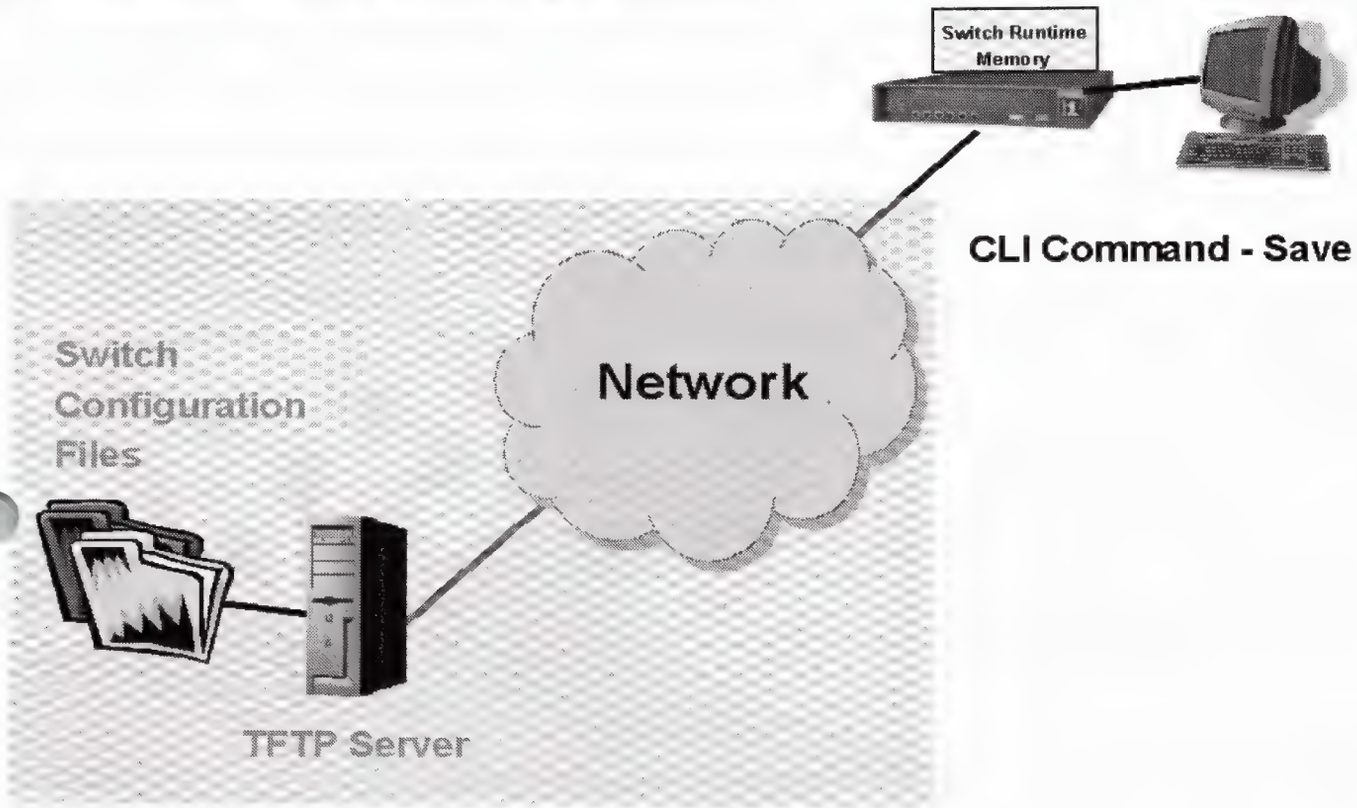
CLI Command – reboot
reboot {cancel | time}
Reboots the switch. The reboot command parameters are as follows:

Time - is the date and time (using a 24-hour clock format) when the switch will be rebooted. Use the following format to enter the date and time: mm/dd/yyyy hh:mm:ss
cancel - is an option used to cancel a previously scheduled reboot.

If you do not specify a reboot time, the reboot happens immediately following the command, and any previously scheduled reboots are cancelled.

© 2001 Extreme Networks,Inc. All rights reserved

Saving the Configuration



Notes:

Returning Switch to Factory Defaults

CLI Command – Unconfig Switch
unconfig switch
Returns the switch to its original factory default settings.

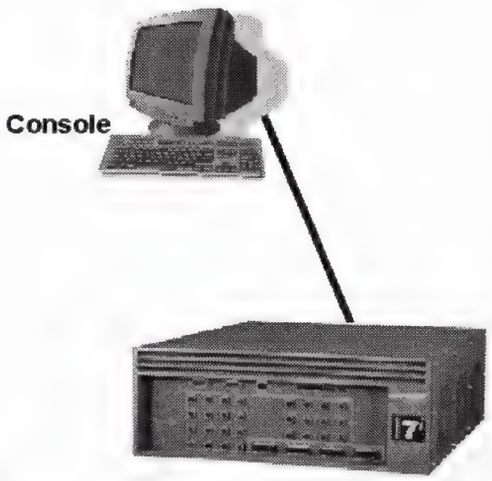
This command resets the entire configuration, with the exception of user accounts and passwords that have been configured, and the date and time.

CLI Command – Unconfig Switch All
unconfig switch all
Resets all parameters except date and time.

NOTE: This command will delete the current selected configuration file.

© 2001 Extreme Networks,Inc. All rights reserved

Returning Switch To Factory Defaults



CLI Command – Unconfig Switch
- Switch is returned to factory defaults, except:
  - User accounts
  - Passwords
  - Date and time

CLI Command – Unconfig Switch all
- Switch is returned to factory defaults, except:
  - Date and time

Notes:

size ≤ 1518

size = 1522, will be dropped.

Switch VLAN - Default

The switch comes with a pre-configured VLAN called “default”. The “default” VLAN has all of the switch ports configured in it. This provides the “plug and play” capability of the Extreme Networks switch family.

For lab exercise purposes, we need to assign an IP address to the pre-configured VLAN “default” so we can then assign an IP address to the PC-laptop that is connected to the switch.

CLI Command – Config VLAN/Unconfig VLAN
config vlan <vlan name> ipaddress <ipaddress> {<netmask>}Assigns or removes an IP address and optional mask to the named VLAN. The mask notation can take either of two forms:

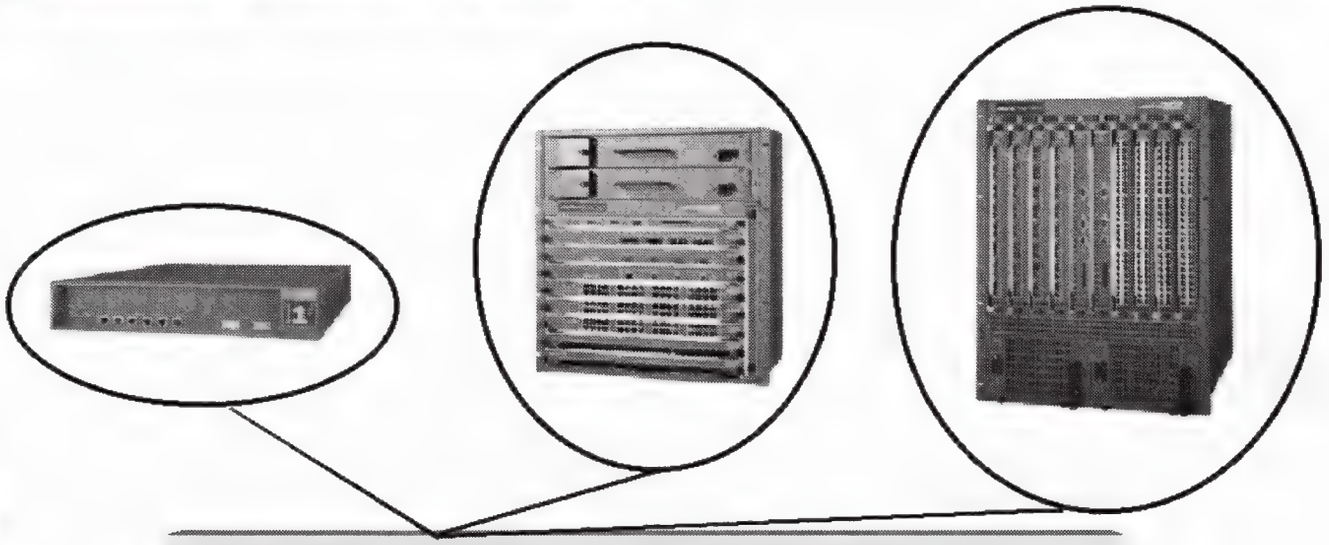
- full dotted-decimal notation , example: 255.255.255.0 or
- slash # notation, example, /24 - which indicates the network portion in binary bits

Examples might be:

- config vlan default ipaddress 10.0.0.1 255.255.255.0
- config vlan default ipaddress 10.0.0.1 / 24

© 2001 Extreme Networks,Inc. All rights reserved

Switch VLAN - Default



- Factory created & pre-configured VLAN
- All ports are automatically members (untagged)
- Need to assign IP address
- "Plug and Play" Capability

Size ≤ 1518

Notes:

What is ExtremeWare Vista?

ExtremeWare Vista is device management software running in a switch. Vista provides a web interface to the switch over a TCP/IP network from a properly configured standard web browser that supports frames and JavaScript (such as NetScape Navigator 3.0 or higher, or MS Internet Explorer 3.0+) for ExtremeWare Vista.

Like most Web Browser Management (WBM) implementations, Vista contains a subset of the available CLI commands. Some of the features not incorporated in Vista are:

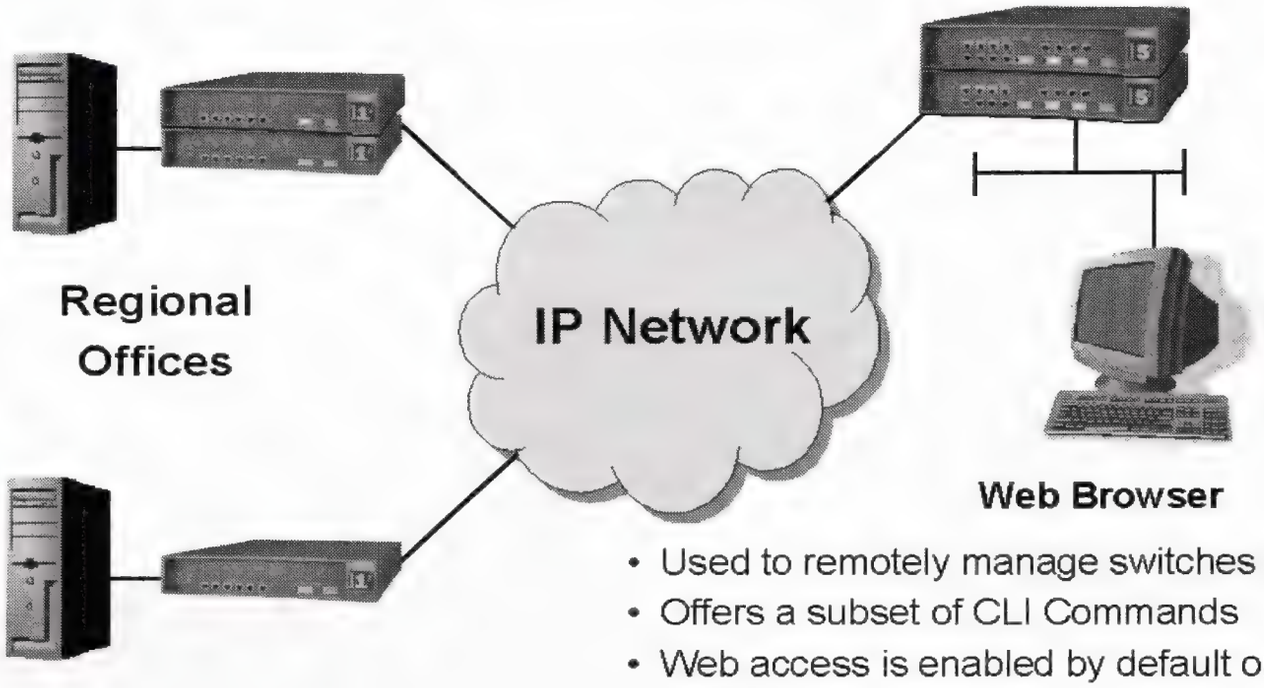
- config upload/download
- port load-sharing
- port mirroring
- clear counters
- show ospf interface
- PIM SM
- ESRP
- IPX
- BGP
- Access lists and profiles

CLI Command – Enable/disable Web
enable/disable web
Enables or disables the web access to the switch. Reboot the switch for the changes to take place. Web access on the switch is enabled by default.

NOTE: To use ExtremeWare Vista, at least one VLAN on the switch must be assigned an IP address.

© 2001 Extreme Networks,Inc. All rights reserved

What is ExtremeWare Vista?



- Used to remotely manage switches
- Offers a subset of CLI Commands
- Web access is enabled by default on
- switch

Notes:

Other Switch Management Tools

In addition to the management functions we have looked at, including the most commonly used CLI commands, ExtremeWare Vista, and how to load and upgrade software and configuration files, the remaining part of this chapter will examine some of the other management features of the switches. These are additional tools that provide enhanced management of the Extreme Networks switch family.

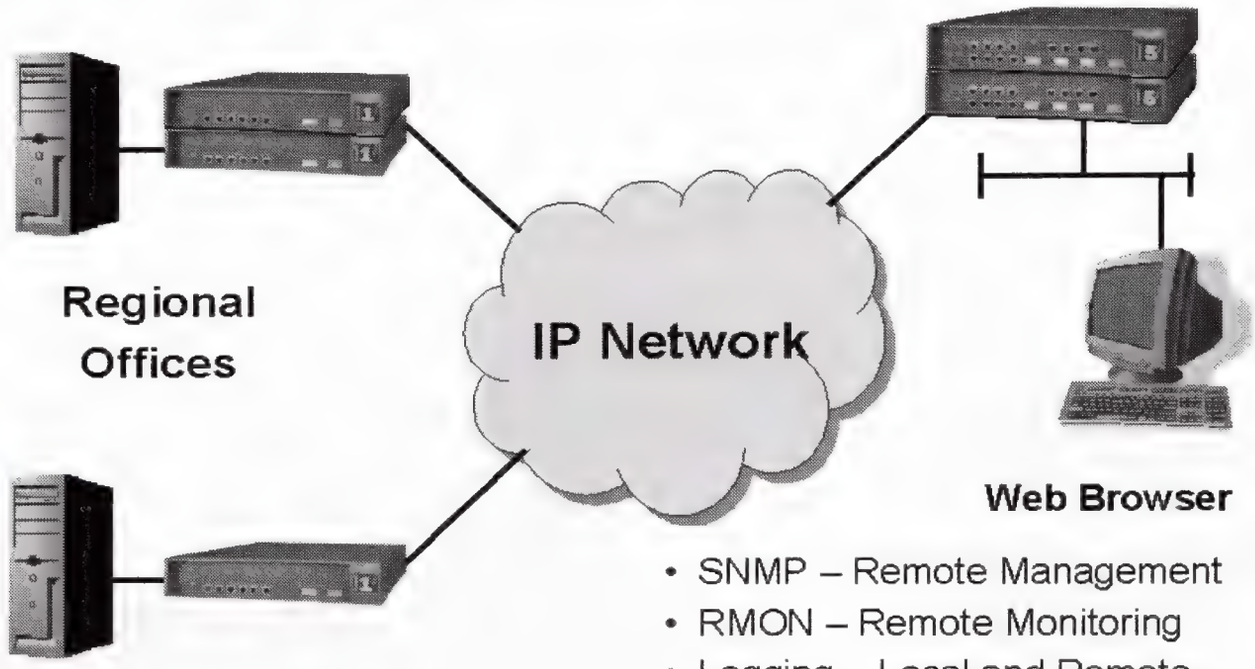
These tools include:

- SNMP
- RMON
- Logging features (local and remote)

For disaster recovery, you can utilise the BootROM menu options.

© 2001 Extreme Networks,Inc. All rights reserved

Other Switch Management Tools



- SNMP – Remote Management
- RMON – Remote Monitoring
- Logging – Local and Remote
- Logging of events

Notes:

Using SNMP

Any Network Manager running SNMP can manage the switch as long as the correct MIBs (Management Information Base) are properly installed on the management console.

Similar to its predecessor, (EEM - Extreme Enterprise Manager) EPICenter is an integrated application suite that simplifies configuration, troubleshooting, and status monitoring of IP-based networks, offering a comprehensive set of network management applications, including the ability to configure, monitor, troubleshoot, and manage the network and its elements.

NOTE: In order to have access to the SNMP agent residing in the switch, at least one VLAN must have an IP address assigned to it.

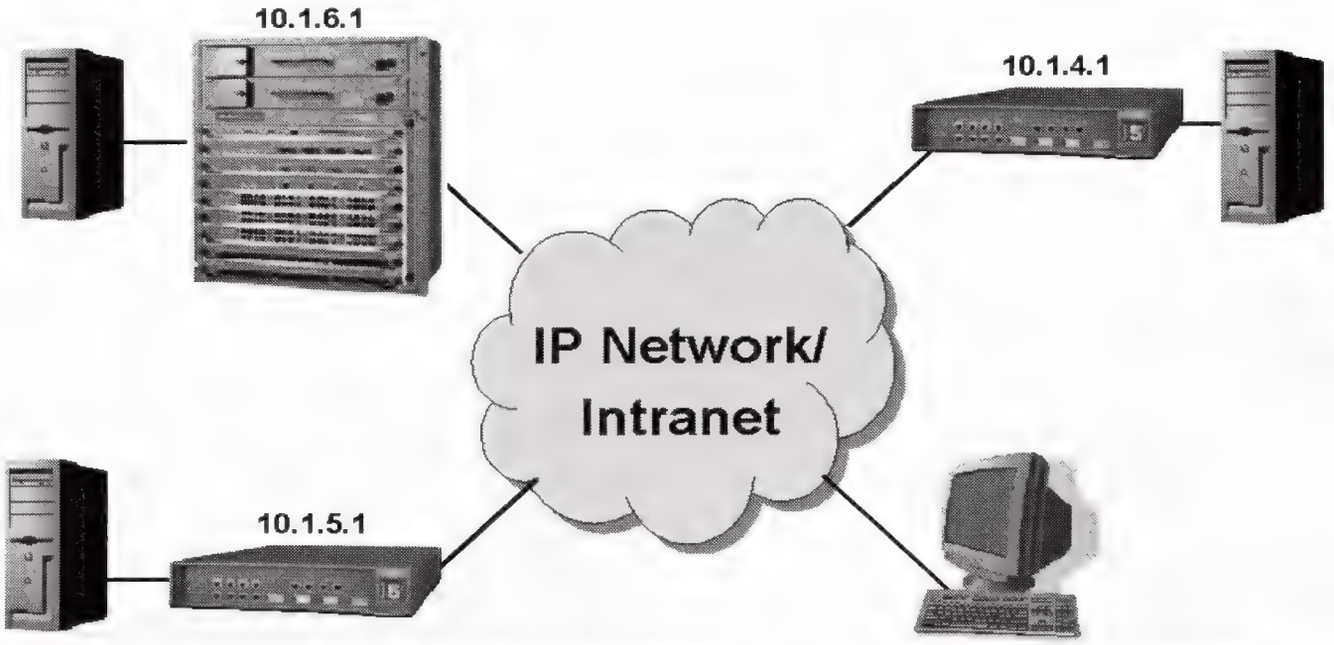
If you can access one VLAN, you can manage the rest of the VLANs, because access to one VLAN gives you access to the entire switch.

As far as Extreme Networks is concerned, the switch is only one device since it only has one MAC address that is shared.

NOTE: Ensure that you install the MIBs correctly!

© 2001 Extreme Networks,Inc. All rights reserved

Using SNMP



- At least one VLAN per switch must have an IP address
- Can then access SNMP agent from management workstation

- Any SNMP based network manager can manage a switch
- Switch MIB must be installed correctly on management workstation

Notes:

SNMP Configuration Parameters

When configuring the SNMP settings, the following SNMP parameters can be configured on the switch:

Authorised Trap Receivers
An authorised trap receiver can be one or more network management stations on your network. The switch sends SNMP traps to all trap receivers. You can have a maximum of sixteen trap receivers configured per switch. Entries in the list can be created, modified, and deleted using the RMON2 trapDesTable MIB variable, as described in RFC 2021.

Authorised Managers
The ability to read and read/write SNMP information can be restricted through the use of an access profile. An access profile permits or denies a named list of IP addresses.

Standard Community Strings
This allows a simple method of authentication between the switch and the remote Network Manager. There are two community strings available on the switch, read/write and read only.

- private = default read/write community string
- public = default read-only community string

System Contact (optional)
This is a text field that enables you to enter the name of the person(s) responsible for managing the switch.

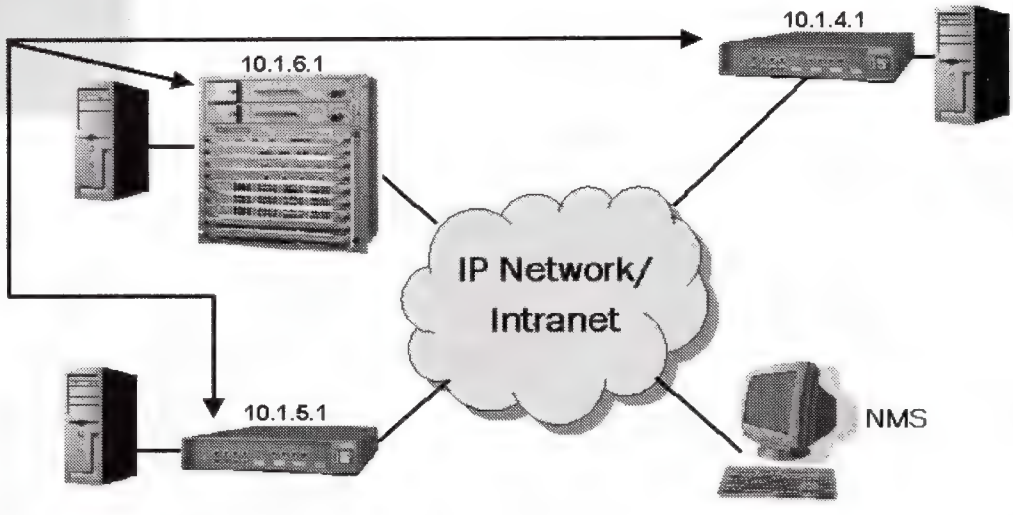
System Name
This is the name that is assigned to this switch. The default name is the model name of the switch (for example, Summit48i).

System Location (optional)
This is a text field that enables you to enter the location of the switch.

© 2001 Extreme Networks,Inc. All rights reserved

SNMP Configuration Parameters

- Authorised trap receivers
- SNMP read access
- SNMP read/write access
- Community strings
- System contact
- System name
- System location



Notes:

SNMP Configuration CLI Commands

The SNMP related CLI commands are listed. For further information please refer to the ExtremeWare Software User Guide for details.

CLI Command – Enable SNMP Access
enable snmp access
Turns on SNMP support for the switch.

CLI Command – Enable SNMP Traps
enable snmp traps
Turns on SNMP trap support.

CLI Commands – Config SNMP Add TrapReceiver
config snmp add trapreceiver <ip_address> community <string>
Adds the ip address of a specified trap receiver. The ip address can be a unicast, multicast, or broadcast address . Maximum of 6 trap receivers.

CLI Command – Config SNMP Community
config snmp community [readonly | readwrite] <string>
Adds an SNMP read or read/write community string. Each community string can have a maximum of 126 characters, and can be enclosed by double quotation marks.

CLI Command – Config SNMP Delete TrapReceiver
config snmp delete trapreceiver [<ip_address> community <string> | all] Deletes the IP address of a specified trap receiver or all authorised trap receivers.

CLI Command – Config SNMP Syscontact
config snmp syscontact <string>
Configures the name of system contact. Maximum 255 characters allowed.

CLI Command – Config SNMP Sysname
config snmp sysname <string>
Configures the name of the switch. Maximum 32 characters allowed. Default sysname is the model name of the device (for example, Summit4). The sysname appears on the prompt.

CLI Command – Config SNMP Syslocation
config snmp syslocation <string>
Configures the location of the switch. A maximum of 255 characters is allowed.

CLI Command – Config SNMP Access Profile
config snmp access-profile [readonly | readwrite] [<access_profile> | none]
Assigns an access profile that limits which stations have read-only or read-write access to the switch.

© 2001 Extreme Networks,Inc. All rights reserved

SNMP Configuration CLI Commands

- enable snmp access
- enable snmp traps
- config snmp add trapreceiver <ip_address> community <string>
- config snmp community [readonly | readwrite] <string>
- config snmp delete trapreceiver [<ip_address> community <string> | all]
- config snmp syscontact <string>
- config snmp sysname <string>
- config snmp syslocation <string>
- config snmp access-profile [readonly | readwrite] [<access_profile> | none]

Notes:

Remote Monitoring - RMON Feature

RMON is a common abbreviation for the Remote Monitoring Management Information base (MIB) system defined by the Internet Engineering Task Force (IETF) documents RFC 1271 and RFC 1757, which allows you to monitor LANs remotely.

A typical RMON setup consists of the following two components:

- RMON probe - An intelligent, remotely controlled device or software agent that continually collects statistics about a LAN segment or VLAN. The probe transfers the information to a management workstation on request, or when a predefined threshold is crossed.

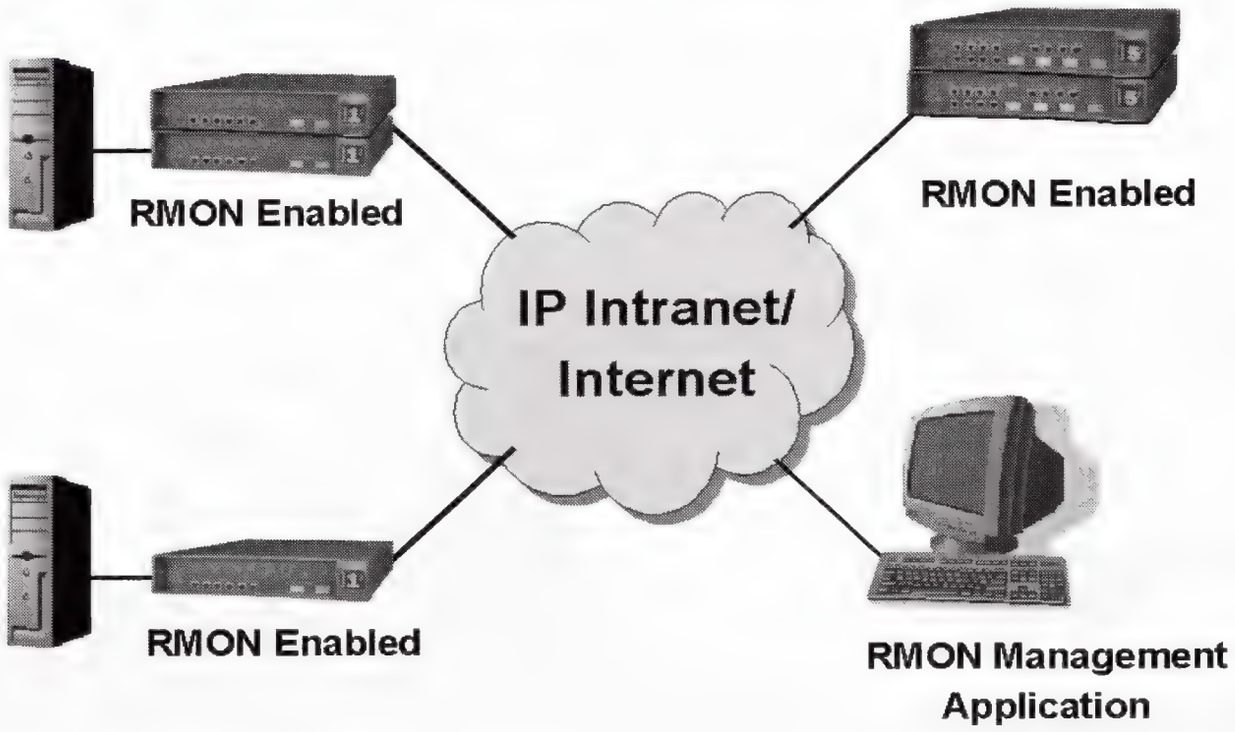
- Management workstation - Communicates with the RMON probe and collects the statistics from it. The workstation does not have to be on the same network as the probe, and can manage the probe by in-band or out-of-band connections.

The Extreme Networks switch RMON capability allows the network administrators to improve system efficiency and reduce the load on the network.

You can only use the RMON features of the system if you have an RMON management application, and have enabled RMON on the switch.

© 2001 Extreme Networks,Inc. All rights reserved

Remote Monitoring - RMON Feature



Notes:

RMON Features of the Switch

The IETF defines 9 groups of Ethernet RMON statistics. RMON Group 10 (which has subgroups) was developed for the Token Ring LAN. Groups 11 through 20 are defined by RMON2 and were developed to capture information up to the application level. The Extreme Networks switch family supports four of the RMON groups. They are Statistics, History, Alarms, and Events.

RMON Ethernet Statistics Group
Provides traffic and error statistics showing packets, bytes, broadcasts, multicasts, and errors on a LAN segment or VLAN. Information from this group is used to detect changes in traffic and error patterns in critical areas of the network

RMON Ethernet History Group
Provides historical views of network performance by taking periodic samples of the counters supplied by the Statistics group. The group features user-defined sample intervals and bucket counters for complete customisation of trend analysis. The history group is useful for analysis of traffic patterns and trends on a LAN segment or VLAN, and to establish baseline information indicating normal operating parameters.

RMON Ethernet Alarms Group
Provides a versatile, general mechanism for setting threshold and sampling intervals to generate events on any RMON variable. Both rising and falling thresholds are supported, and thresholds can be on the absolute value of a variable or its delta value. In addition, alarm thresholds may be auto-calibrated or set manually. Alarms inform you of a network performance problem and can trigger automated action responses through the Events group.

RMON Ethernet Events Group
Creates entries in an event and/or sends SNMP traps to the management station. An event is triggered by an RMON alarm. The action taken can be configured to ignore it, to log the event, to send an SNMP trap to the receivers listed in the trap receiver table, or to both log and send a trap. Ref. RFC 1757.

NOTE: Non-supported RMON Groups are Hosts, Host Top N, Matrix, Filters, and Capture.

© 2001 Extreme Networks,Inc. All rights reserved

RMON Features of the Switch

IETF
RMON Functional Hosting

1. Statistics 2. History	4. Hosts 5. Host Top N 6. Matrix
3. Alarms 9. Events	7. Filters 8. Capture
10. Token Ring Groups	
11-20. RMON 2	

RMON features of the Switch

- Ethernet Statistics Group
- Ethernet History Group
- Ethernet Alarms Group
- Ethernet Events Group

Notes:

Configuring RMON and Event Actions

RMON requires one probe per LAN segment, and standalone RMON probes have traditionally been expensive. Therefore, Extreme Network's approach has been to build an inexpensive RMON probe into the agent of each system.

This allows RMON to be widely deployed around the network without costing more than traditional network management. The switch accurately maintains RMON statistics at the maximum line rate of all of its ports. For example, statistics can be related to individual ports.

In addition, because a probe must be able to see all traffic, a stand-alone probe must be attached to a non-secure port. Implementing RMON in the Extreme Networks switch means that all ports can have security features enabled.

CLI Command - Enable/disable RMON
[enable | disable] rmon
Allows you to enable or disable the collection of RMON statistics on the switch. By default, RMON is disabled. However, even in the disabled state, the switch responds to RMON queries and sets for alarms and events. By enabling RMON, the switch begins the processes necessary for collecting switch statistics.

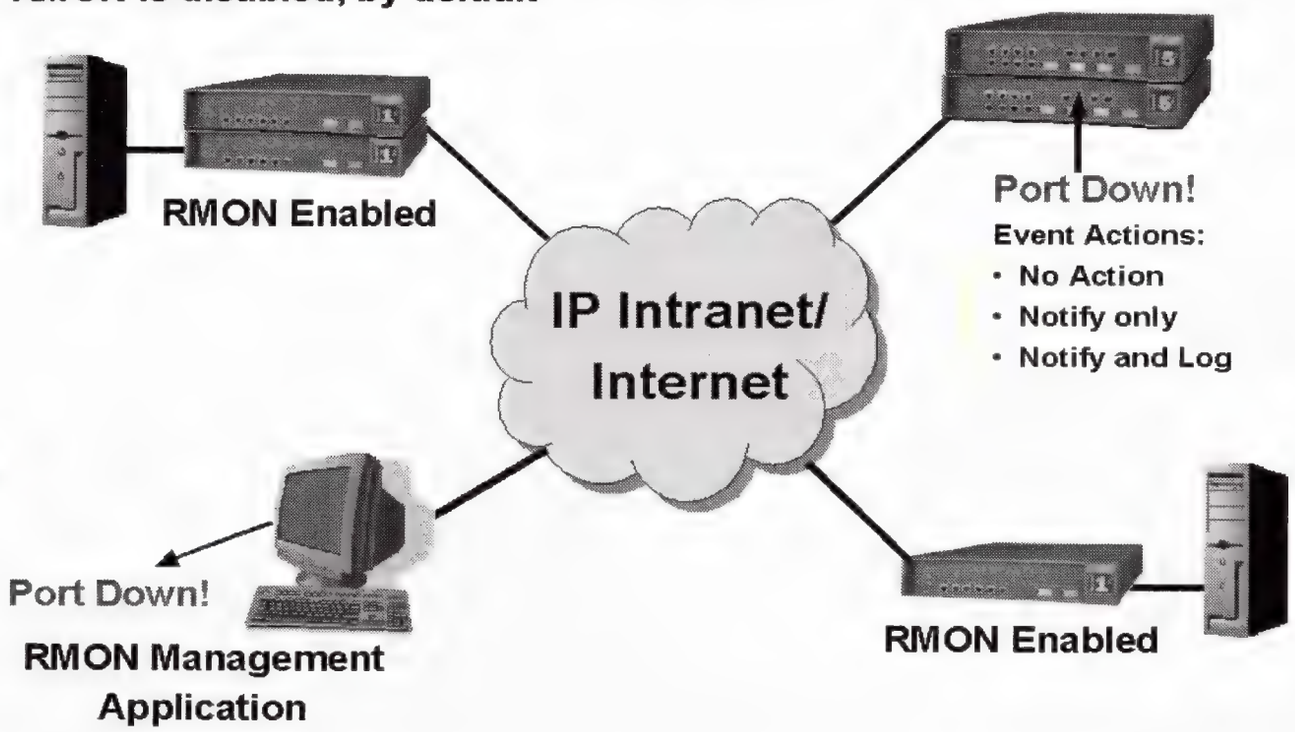
The actions that you can define for each alarm are: No action, Notify only and Notify and log. To be notified of events using SNMP traps, configure one or more trap receivers.

NOTE: This can only be configured from the management station through SNMP.

© 2001 Extreme Networks,Inc. All rights reserved

Configuring RMON and Event Actions

RMON is disabled, by default



Notes:

Logging Features

The switch's log tracks all configuration and fault information pertaining to the device. Each entry in the log contains the following information:

Timestamp
The timestamp records the month and day of the event, along with the time (hours, minutes, and seconds) in the form HH:MM:SS. If the event was caused by a user, the user name is also provided.

Fault Level
Describes the four levels of importance that the switch can assign to a fault. Critical, Warning, Informational and Debug. By default, log entries that are assigned a critical or warning level remain in the log after a switch reboot. Issuing a clear log command does not remove these static entries.

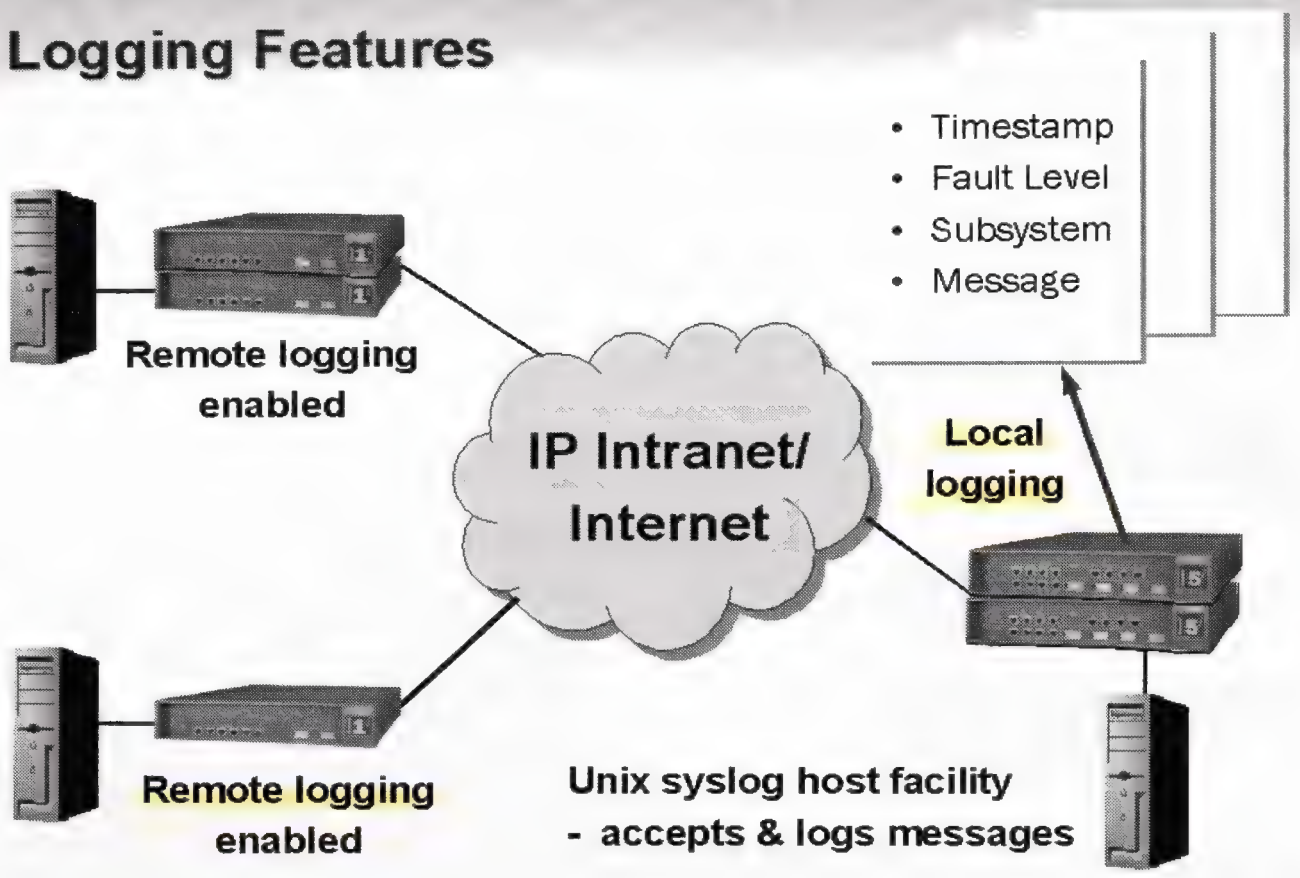
Subsystem
The facility flags one of seven specific functional areas of the switch to which the error refers.

Message
The message contains the log information with text that is specific to the problem.

CLI Command – Clear Log
clear log static
Removes the log entries of all levels (including warning or critical).

© 2001 Extreme Networks,Inc. All rights reserved

Logging Features



Notes:

Configure Logging

Remote Logging

In addition to maintaining an internal log, the switches support remote logging by way of the UNIX Syslog host facility. To enable remote logging, perform the tasks of configuring the Syslog host to accept and log messages, and enable remote logging.

CLI Command – Enable Syslog

enable syslog

The command enable syslog enables remote logging.

CLI Command – Config Syslog

config syslog <ipaddress> <facility> {<priority>}

Configures remote logging. You will need to specify the following:

ipaddress - the ip address of the syslog host.

facility - The syslog facility level for local use. Options include local0 through local7.

priority - Filters the log to display message with selected priority or higher (more critical). Priorities include (in order) critical, emergency, alert, error, warning, notice, info, and debug. If not specified, debug priority messages and higher are displayed.

Local Logging

CLI Command – Show Log

show log {<priority>}

Allows you to display a snapshot of the log at any time. The priority parameter filters the log to display messages with selected priority or higher (more critical). Priorities include (in order) critical, emergency, alert, error, warning, notice, info, and debug. If not specified, debug priority messages, and higher, are displayed. The switch maintains 1,000 messages in its internal log.

CLI Command – Enable Log Display

enable log display

Enables a running real time display of log messages to the console.

CLI Command – Configure Log Display

config log display {<priority>}

Configures the log display, if a priority is not specified, only messages of critical priority are displayed.

CLI Command – Enable CLI Config Logging

enable cli-config-logging

Enables logging of any configuration changes.

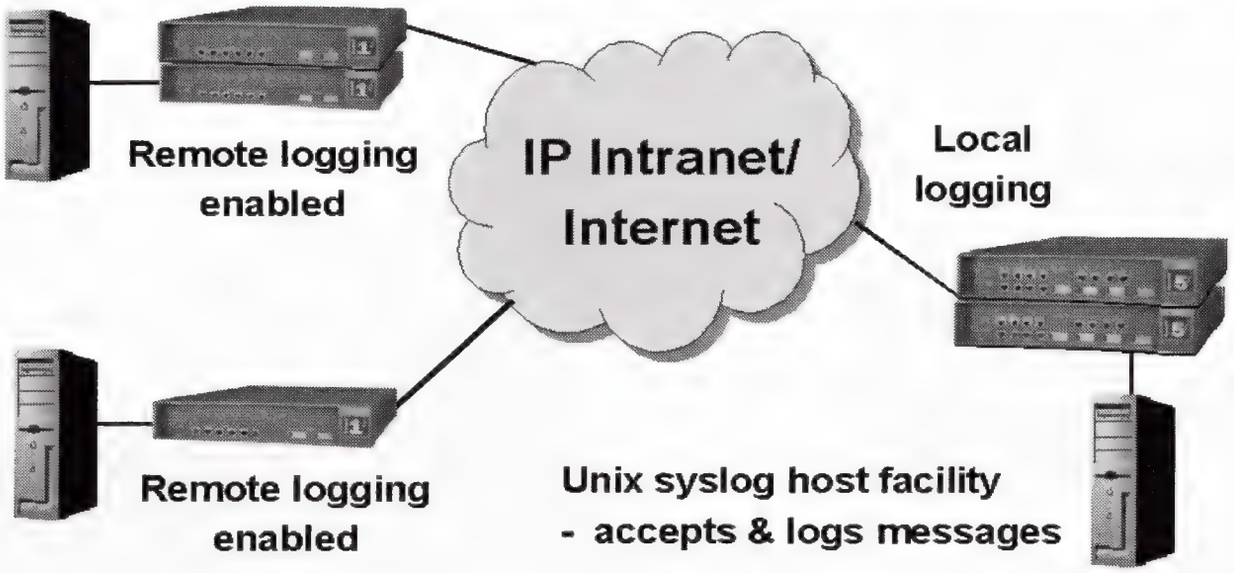
NOTE: You can enable the real time log display via a Telnet session, however, the real time logging will only be displayed on the local console.

© 2001 Extreme Networks,Inc. All rights reserved

Configure Logging

Enable remote logging
Using CLI commands:
- enable syslog
- configure syslog<ipaddress><facility>{<priority>}

Local logging
- 1000 messages in Switch's internal log
- display log snapshot anytime with CLI command:
- show log {<priority>}



Notes:

The Switch BootROM

The BootROM of the switch initialises certain important switch variables during the boot process. If necessary, BootROM can be upgraded, after the switch has booted, using TFTP. For disaster recovery purposes (i.e. in the event the switch does not boot properly), some boot option functions can be accessed through a special BootROM menu.

CLI Command – Download BootROM
download bootrom <hostname / IP>
The command download bootrom allows you to upgrade the BootROM from a specified host system.

NOTE 1: Reboot the switch after downloading the BootROM.

NOTE 2: First upgrade the BootROM, reboot the switch and then upgrade the software image.

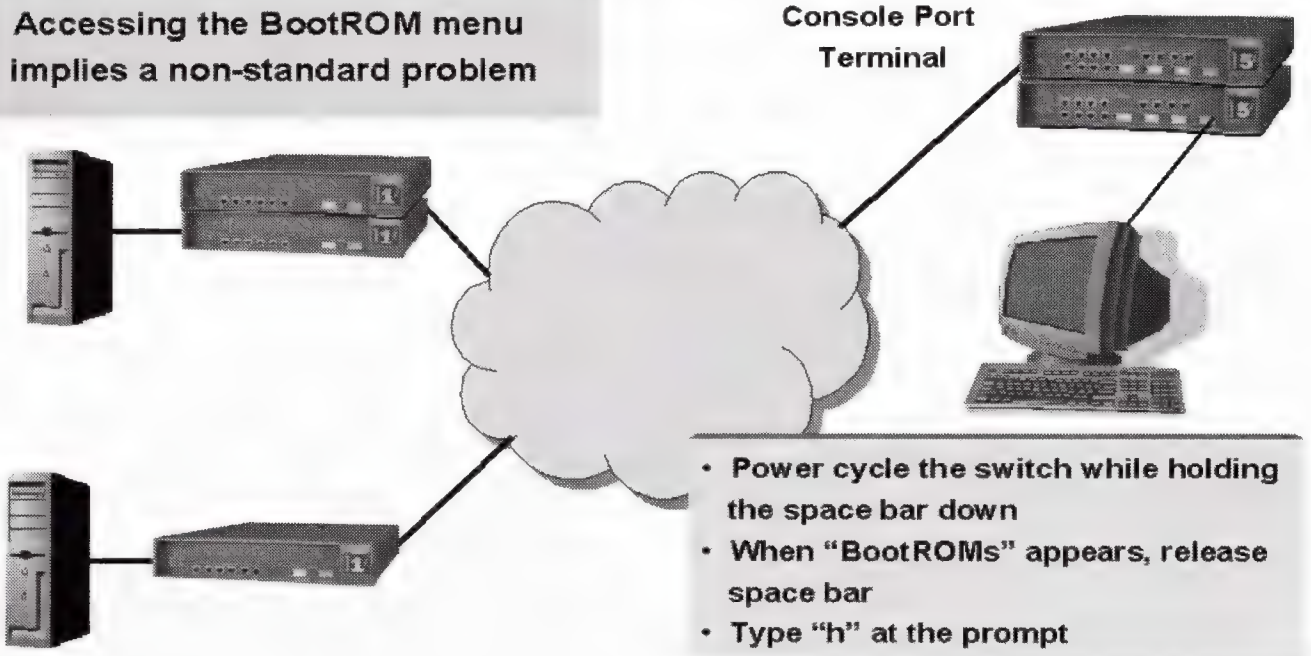
NOTE 3: Software v6.1.9b11 requires BootROM v7.2.

© 2001 Extreme Networks,Inc. All rights reserved

The Switch BootROM

Extreme Support Assistance Required

Accessing the BootROM menu implies a non-standard problem



- Power cycle the switch while holding the space bar down
- When "BootROMs" appears, release space bar
- Type "h" at the prompt

Notes:

BootROM Menu Options

The slide shows the options available from the switch's BootROM menu after entering the help command (or "h").

NOTE: Option p is not used at this time.

Interaction with the BootROM menu is only required under special circumstances and should be done only under the direction of Extreme Networks Customer Support. The necessity of using these functions implies a non-standard problem, which requires the assistance of Extreme Networks Customer Support.

The BootROM Menu can only be accessed when the switch is hard-booted.
When asked to depress the <spacebar> remember to:

Hold the <spacebar> key, not press it!

© 2001 Extreme Networks,Inc. All rights reserved

BootROM Menu Options

BootROM-> h

1: Select primary code image
2: Select secondary code image
3: Select primary configuration
4: Select secondary configuration
b: Change baud rate
d: Force default configuration = unconfig (switch all)
f: Boot on board flash
h: Help
k: Erase selected configuration
p: Boot PCMCIA card
s: Load code image from serial port using XMODEM
BootROM->

Notes:

Summary

Chapter three has provided an introduction to the Extreme Networks switch management functions and configuration procedures. You should now be able to:

- Describe ExtremeWare Management & Security
- Describe CLI structure and organisation
- Explain basic CLI commands such as create, config, enable and show
- Define ExtremeWare software, switch boot images and configuration files
- Utilise CLI commands - download, upload, and use
- Define and configure the VLAN "Default"
- Explain the use of additional management tools – SNMP, RMON, Logging and BootROM
- Successfully complete the lab exercises

© 2001 Extreme Networks,Inc. All rights reserved

Summary

You should now be able to:

- **Describe ExtremeWare Management & Security**
- **Describe CLI structure and organisation**
- **Describe CLI Basic commands- create, config, enable and show**
- **Define ExtremeWare software, switch boot images and configuration files**
- **Utilise CLI commands - Download, Upload, & Use**
- **Define and configure the VLAN "Default"**
- **Discuss additional management tools – SNMP, RMON, Logging and BootROM**
- **Successfully complete the lab exercises**

Notes:

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 4

Port Configuration

Chapter Objectives

Chapter four provides you with an examination of the different types of ports supported in the Extreme Networks switch family, including the configurable port parameters.

Upon completion of this chapter, you will be able to:

- Describe the port configuration CLI commands
- Define the load sharing feature and its benefits
- Explain the Extreme Discovery Protocol (EDP)
- Successfully complete the lab exercises

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

Upon completion of this chapter, you will be able to:

- **Describe the port configuration CLI commands**
- **Define the load sharing feature and its benefits**
- **Explain the Extreme Discovery Protocol (EDP)**
- **Successfully complete lab exercises**

Notes:

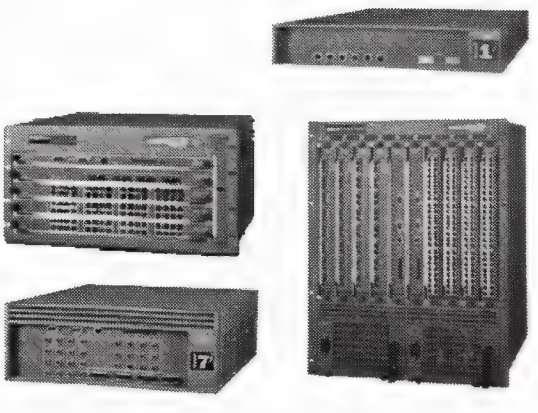
Switch Port Types

Depending on the switch configuration, a Summit, Alpine or BlackDiamond switch is capable of supporting a variety of port types listed in the slide.

© 2001 Extreme Networks,Inc. All rights reserved

Switch Port Types

- **10/100 Base-T (Ethernet and Fast Ethernet)**
- **100Base-FX (Fast Ethernet over Fibre)**
  - SC or MT-RJ-based → one single connector
    two connectors
- **100/1000Base-T (Fast and Gigabit Ethernet)**
- **1000Base-X**
  - SX,LX or LX-70 GBIC-based
    small < Long
  - MT-RJ-based GBIC-based
  - Gigabit Ethernet over Fibre



Notes:

Configurable Port Parameters

Summit Switches
Ports on the Summit switch can be configured in the following ways:

- Enabling and disabling individual ports
- Configuring the port speed
- Configuring half- or full-duplex mode
- Disabling auto-negotiation for Gigabit port
- Creating load-sharing groups on multiple ports
- Configuring QoS on a port-by-port basis

BlackDiamond and Alpine Switches
For ports on the BlackDiamond or Alpine switch, the port number is a combination of the slot number and th port number. The nomenclature for the port number is as follows:

slot: port

An example might be: port 4 of an I/O module installed in slot 2 which would be identified as port number 2:4.

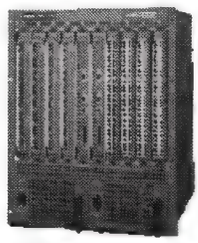
You can also use wildcard combinations (*) to specify multiple BlackDiamonds or Alpine slot and port combinations. (The three commands config slot, clear slot and show slot are applicable only for the chassis-based switches).

CLI Command – Enable/disable Port
[enable | disable] ports [all] <port number>
Enables and disables one or more ports. By default, all ports are enabled.
Even though a port is disabled, the link remains enabled for diagnostic purposes. The port status LEDs will flash green when a link is present and the port is disabled.
Please refer to the ExtremeWare Software User Guide 6.1+ for more details about configuring the Alpine an BlackDiamond switches.

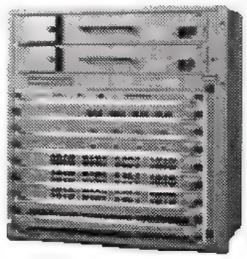
© 2001 Extreme Networks,Inc. All rights reserved

Configurable Port Parameters

BlackDiamond and Alpine Switches



- **When configuring port numbers, use this nomenclature:**
  - SLOT : PORT NUMBER
  - Example: 2:4
    - Represents port 4 in an I/O module installed in Slot 2
- **Configure/use the type of I/O module installed per slot using CLI commands**
  - config slot <slot number> module [f32f | f48t | g4x | g8x]
    - *Modules shown may vary on type of switch.*
  - clear slot
  - show slot



Notes:

Auto-negotiation, Speed and Duplex

The switch is configured to use auto-negotiation to determine the port speed and duplex setting for each port.

- Fast Ethernet ports can be manually configured for either 10Mbps or 100Mbps
- Fast Ethernet ports can be configured for half- or full-duplex operation
- 100BASE-FX ports operate in full-duplex only and the speed cannot be modified
- Gigabit fibre Ethernet ports are statically set to 1 Gbps and their speed cannot be modified

Duplex and speed settings can be manually configured for 10/100 or 100/1000 Mbps copper ports.

Gigabit fibre ports are statically set to 1 Gbps, and speed and duplex mode cannot be modified.

Flow control for Gigabit Ethernet ports is supported, and is enabled or disabled as part of auto-negotiation:

- disabled if auto-negotiation is turned off
- enabled if auto-negotiation is turned on

Turning Off Auto-Negotiation – Gigabit Ethernet
In certain interoperability situations, it is necessary to turn auto-negotiation off on a Gigabit Ethernet port. Even though a Gigabit fibre port runs only at full duplex and gigabit speeds, the command that turns off auto-negotiation must still include the duplex setting.

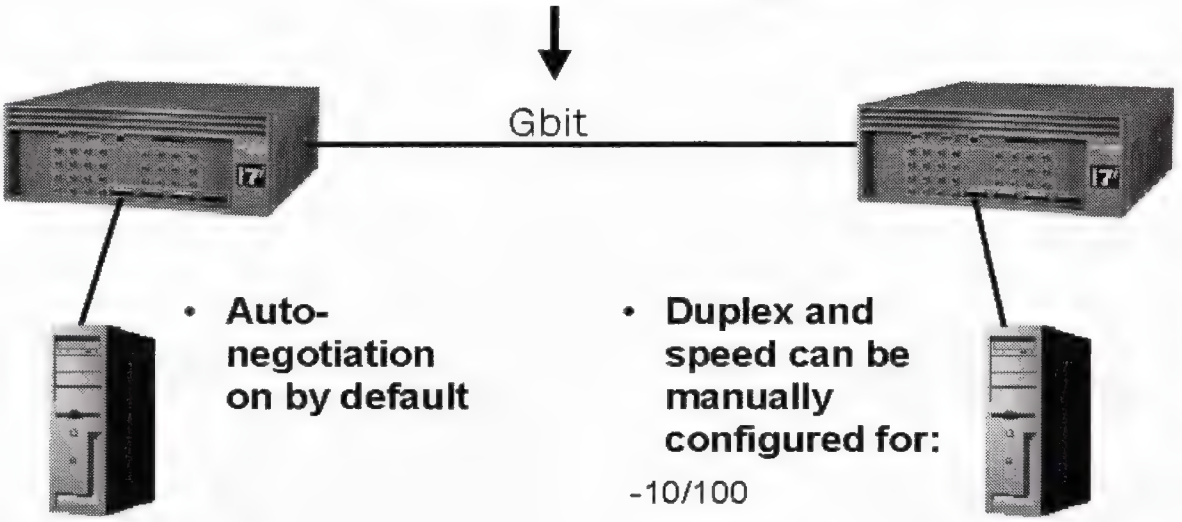
An example of turning auto-negotiation off for port 49 (a Gigabit fibre port) is:
config port 49 auto off duplex full

CLI Command – Configure Port
config ports [all | <port number>] auto [off | on] <duplex [full | half]> <speed [10 | 100 | 1000]>
Configures ports for auto-negotiation, duplex and speed.

© 2001 Extreme Networks,Inc. All rights reserved

Auto-negotiation, Speed and Duplex

- Flow control supported
- Can turn off auto-negotiation



- Auto-negotiation on by default
- Duplex and speed can be manually configured for:
  - -10/100
  - -100/1000

Note: Gbit is always Full-Duplex

Notes:

auto ↔ auto (not good)

auto off - light on

Jumbo Frames

Ethernet frames that are larger than 1522 bytes, (1514 + 4 bytes 802.1Q tag + 4 bytes CRC) are called *Jumbo Frames*.

Extreme Networks switches, of the i-series chipset, support switching and routing of jumbo frames at wire-speed on all ports.

Jumbo frames are used between endstations that support larger frame sizes for more efficient transfers of bulk data. Both endstations involved in the transfer must be capable of supporting jumbo frames. This is because the switch does not perform IP fragmentation, or participate in MTU negotiation on behalf of devices that do not support jumbo frames.

NOTE: Some network interface cards (NICs) have an MTU size that does not include the 4-byte CRC. You must ensure that the NIC MTU size is at or below the maximum MTU size configured on the switch. Frames that are larger than the MTU size configured are dropped at the ingress port.

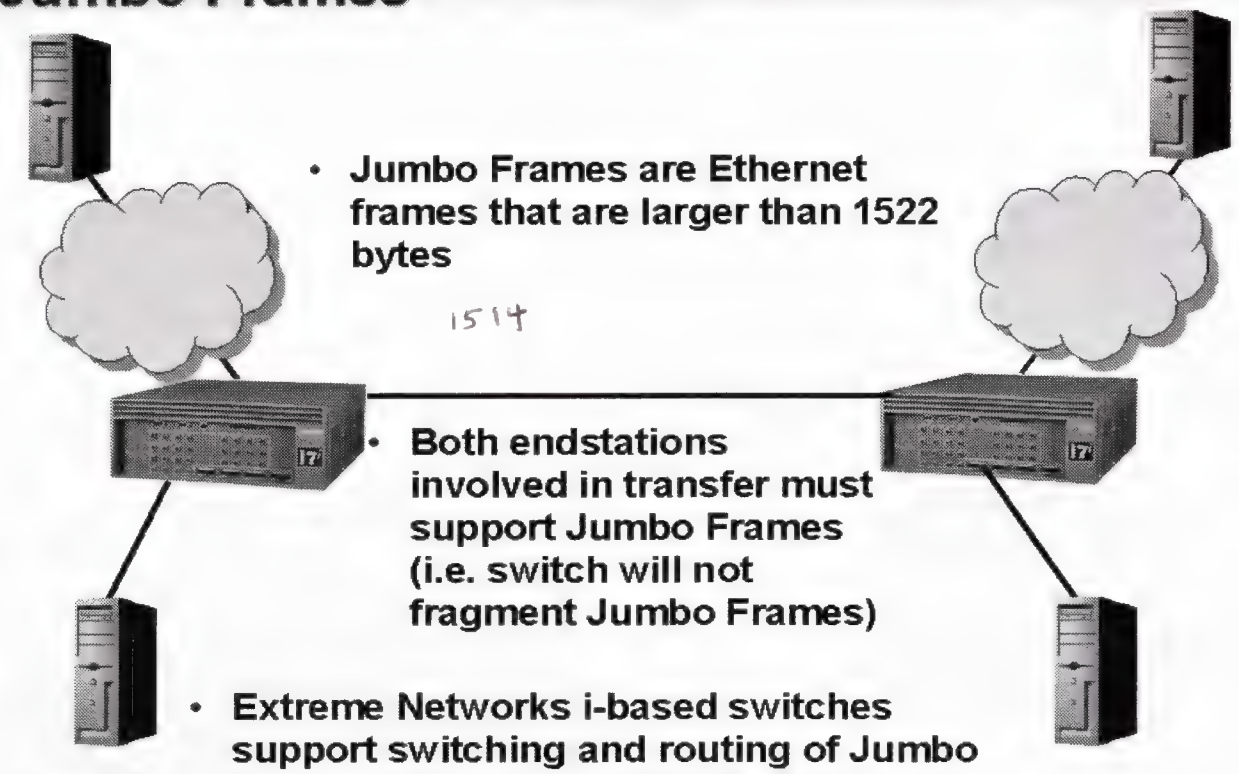
To enable support for jumbo frames, you must configure the maximum MTU size of the jumbo frame allowed by the switch (ranges from 1523 – 9216). > 9216

CLI Command – Config Jumbo Frame Size
config jumbo-frame size <jumbo_frame_mtu>
Configures the maximum MTU size allowed by the switch.

CLI Command – Enable Jumbo Frame
enable jumbo-frame ports [all | <ports list>]
Enables support on ports that will carry jumbo frames.

© 2001 Extreme Networks,Inc. All rights reserved

Jumbo Frames



- Jumbo Frames are Ethernet frames that are larger than 1522 bytes

1514

- Both endstations involved in transfer must support Jumbo Frames (i.e. switch will not fragment Jumbo Frames)
- Extreme Networks i-based switches support switching and routing of Jumbo Frames at wire speed on all ports

802.1P
802.1Q
high priority

Notes:

Port Load Sharing Feature

Load sharing allows you to increase bandwidth and resilience between Extreme Networks switches by using a group of ports to carry traffic in parallel between switches. The sharing algorithm allows the switch to use multiple ports as a single logical port. For example, VLANs see a load-sharing group as a single logical port. Most load sharing algorithms guarantee packet sequencing between clients.

If a port in a load-sharing group fails, traffic is redistributed to the remaining ports in the load-sharing group. If the failed port becomes active again, traffic is redistributed to include that port.

NOTE: Load sharing must be enabled on both ends of the link, or a network loop will result.

In the situation where the port based algorithm is the only type of load-sharing possible, (on non-i switches) it can be used to great effect where the traffic transmitted from the switch to the load-sharing group is sourced from an equal or greater number of ports on the same switch. For example, traffic transmitted to a 2-port load-sharing group should originate from a minimum of two other ports on the same switch.

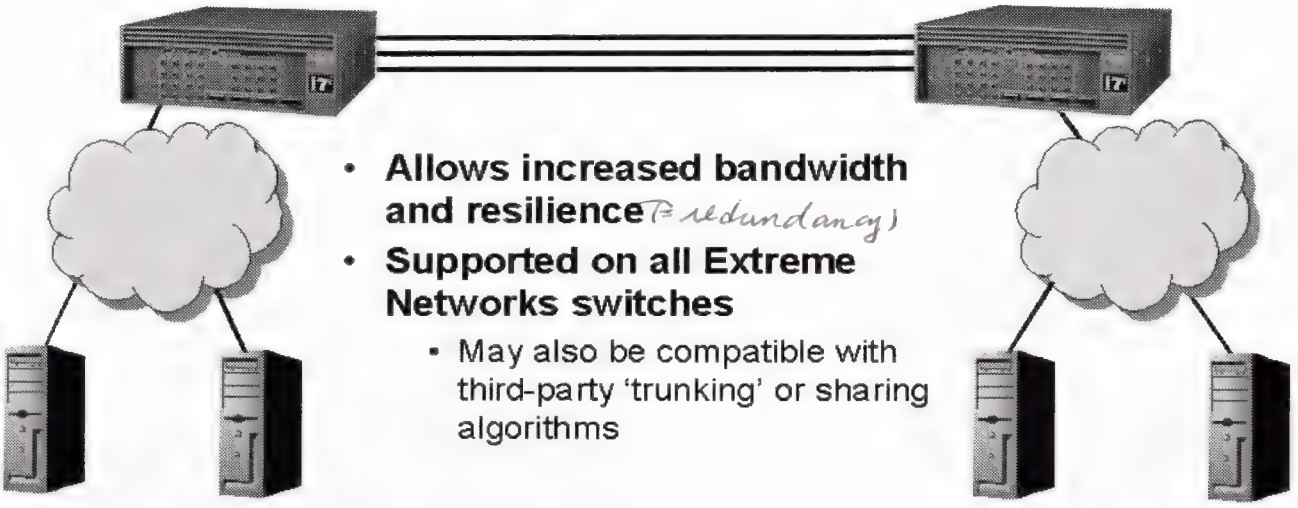
The load-sharing feature is supported between all Extreme Networks switches, and may also be compatibl with third-party "trunking" or sharing algorithms.

NOTE: BlackDiamond trunks cannot span I/O modules.

© 2001 Extreme Networks,Inc. All rights reserved

Port Load Sharing Feature

- **Allows switch to use multiple ports as if a single logical port**
  - aka 'trunking'



- **Allows increased bandwidth and resilience** (= redundancy)
- **Supported on all Extreme Networks switches**
  - May also be compatible with third-party 'trunking' or sharing algorithms

Notes:

Spanning tree — one Link — what ports to block

Port Load sharing — 3 links (in this case)

diverse Link -

goes to different direction

Load Sharing Algorithms

Load-sharing algorithms allow you to select the distribution technique used by the load-sharing group to determine the output port selection.

You can configure three LS algorithms:

Port-based
Uses the ingress port to determine which member port to forward traffic out of the switch. This is a static mapping between ingress port and load-share port.

Address-based
Uses addressing information based on packet protocol, as follows:

- IP packets - Uses source/destination MAC and IP address, and TCP port number
- IPX packets - Uses source/destination MAC address, and IPX network identifiers
- All other Packets - Uses source/destination MAC address

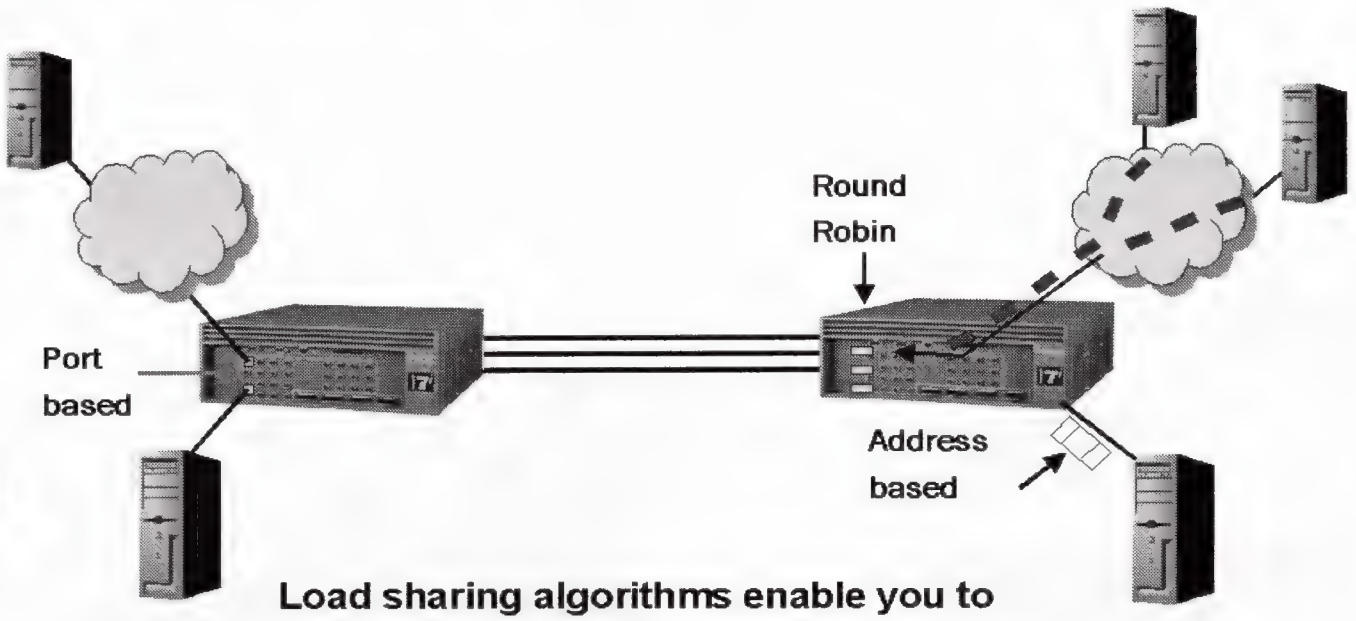
Round-robin
Used when the switch receives a stream of packets, it forwards one packet out of each physical port in the load-sharing group using a round-robin scheme.

NOTE: Using the R-R algorithm, packet sequencing between clients is not guaranteed.

NOTE: If you do not explicitly select an algorithm, the port-based scheme is used as default algorithm. However, the address-based load-sharing algorithm is recommended because it has a more even distribution.

© 2001 Extreme Networks,Inc. All rights reserved

Load Sharing Algorithms



Load sharing algorithms enable you to choose the traffic distribution technique to determine the output port selection

Notes:

sliding windows

timer:

Possible BD Load-Sharing Port Groups for nin "i" based I/O Modules

Load Sharing Rules

To set up the switch to load share among ports, you must create a load-sharing group of ports. Load-sharing groups are defined according to the rules detailed below.

These rules apply for non-i based switches and BlackDiamond I/O modules that do not have the i-chipset:

- Ports on the switch are divided into groups of two or four. You can load-share 2 or 4 links
- Ports in a load-sharing group must be contiguous
- Only port-based algorithm applies
- The first port in the load-sharing group is configured to be the "master" logical port. This is the reference port used in configuration commands. It can be thought of as the logical port representing the entire port group
- Open implementation - compatible with Sun Quad fast Ethernet card and supports Cisco EtherChannel (i-chipset switches only)

These rules apply for BlackDiamond I/O modules that have the i-chipset:

- One group can contain up to 8 ports
- Ports in the group must be on the same module
- Ports in the group do not need to be contiguous

Possible BlackDiamond Load-Sharing Port Groups

The available and valid port combinations for the BlackDiamond non-i based module are shown in the slide. To define a load-sharing group, you assign a group of ports to a single, logical port number.

CLI Command – Enable Sharing

enable sharing <master_port> grouping <portlist>[<cr> | algorithm [address-based | port-based | round-robin]

Enables a load-sharing group.

CLI Command – Disable Sharing

disable sharing <master_port>

Disables a load-sharing group.

CLI Command – Show Ports Configuration

show ports configuration

Use this command to verify a properly configured load-sharing configuration, and the master logical port identity.

© 2001 Extreme Networks,Inc. All rights reserved

Possible BD Load-Sharing Port Groups for non "i" based I/O modules

Table 3-2: Port Combinations for the G4X Module

Load-Sharing Group	1	2	3	4
4-port groups	x	x	x	x
2-port groups	x	x	x	x

Table 3-3: Port Combinations for the G6X Module

Load-Sharing Group	1	2	3	4	5	6
4-port groups	x	x	x	x		
2-port groups	x	x	x	x	x	x

master port

Table 3-4: Port Combinations for the E42T and E32F Modules

Load-Sharing Group	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
4-port groups	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2-port groups	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Load-Sharing Group	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
4-port groups	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2-port groups	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Notes:

Port-Mirroring Feature

Port-mirroring configures the switch to copy all traffic associated with one or more ports to a monitor port on the switch. The monitor port can be connected to a network analyser or RMON probe for packet analysis. The switch uses a traffic filter that copies traffic to the monitor port.

The traffic filter can be defined based on one of the following criteria:

- Physical port - All data that traverses the port, regardless of VLAN configuration, is copied to the monitor port
- VLAN - All data to and from a particular VLAN, regardless of the physical port configuration, is copied to the monitor port
- Virtual port - All data specific to a VLAN on a specific port is copied to the monitor port
- Up to eight mirroring filters and one monitor port can be configured on the switch. Once a port is specified as a monitor port, it cannot be used for any other function

NOTE: Frames that contain errors are not mirrored, and on non-i chipset switches, mirrored frames that are transmitted from the switch do not contain 802.1Q VLAN tagging information.

Port-mirroring commands are described as follows:

CLI Command – Enable Mirroring
enable mirroring to port <port number> [tagged | untagged]
Dedicates a port to be the mirror output port.

CLI Command – Configure Mirroring
config mirroring add [ports<port number> | vlan <vlan name> | vlan <vlan name> ports <port number>]
Adds a single mirroring filter definition from a VLAN, physical port or a specific VLAN/port combination. Up to 8 mirroring definitions can be added.

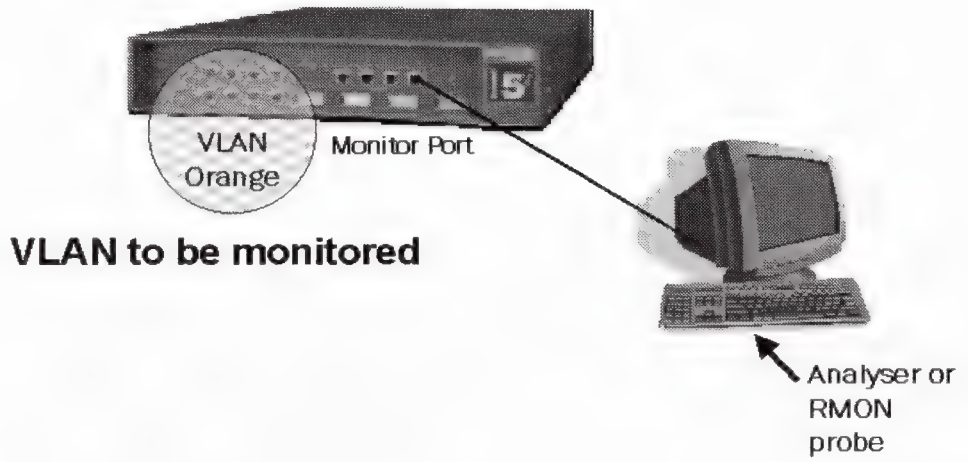
CLI Command – Configure Mirroring
config mirroring delete [ports<port number> | vlan <vlan name> | vlan <vlan name> ports <port number>]
Deletes a particular mirroring filter definition, or all mirroring filter definitions.

CLI Command – Disable Mirroring
disable mirroring
Disables port-mirroring.

CLI Command – Disable Mirroring
show mirroring
Allows you to verify the parameter settings by displaying the port-mirroring configuration.

© 2001 Extreme Networks,Inc. All rights reserved

Port-Mirroring Feature



Errored frames are not mirrored!

Notes:

Extreme Discovery Protocol - EDP

The Extreme Discovery Protocol (EDP) is a Layer 2 protocol and is Extreme Networks proprietary. EDP uses an Ethernet SNAP (Sub-Network Address Protocol) encapsulation and has a destination MAC address of 00-E0-2B-00-00-00. EDP is enabled by default.

EDP is used by the switches to exchange topology information with each other. Information communicated using EDP includes the following:

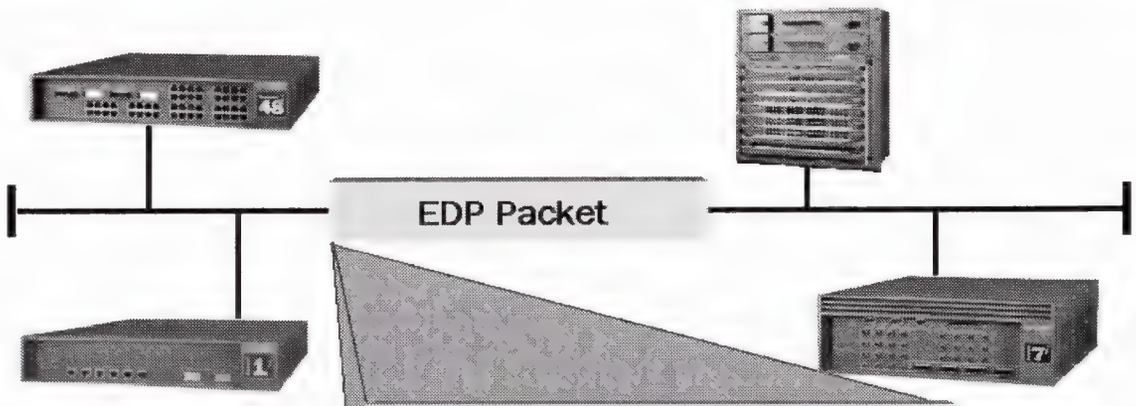
- Switch MAC address (Switch ID)
- Switch software version information
- Switch IP Address,
- Switch VLAN-IP information
- Switch port number

CLI Command - Enable/disable edp Ports
enable/disable edp ports [all | <port number]
Enables or disables the generation and processing of EDP messages on one or more ports.

CLI Command - Show EDP
show edp
Allows verification of EDP parameter settings by displaying EDP information.

© 2001 Extreme Networks,Inc. All rights reserved

Extreme Discovery Protocol - EDP



Proprietary Extreme L2 protocol used for:

-information gathering

-exchanging topology information

- **Switch ID**
- **Switch software version**
- **Switch IP address**
- **Switch VLAN-IP information**
- **Switch Port Number**

Notes:

Summary

Chapter four has provided an introduction to the Extreme Networks switch port types, port parameters and port configuration CLI commands. You should now be able to:

- Describe the port configuration CLI commands
- Define the load sharing feature and its benefits
- Explain the Extreme Discovery Protocol (EDP)
- Successfully complete the lab exercises

© 2001 Extreme Networks,Inc. All rights reserved

Summary

You should now be able to:

- **Describe the port configuration CLI commands**
- **Define the load sharing feature and its benefits**
- **Explain the Extreme Discovery Protocol (EDP)**
- **Successfully complete lab exercises**

Notes:

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 5

Bridging Overview and Configuration

Chapter Objectives

Chapter five provides you with an overview of the different bridge types, a definition and an operational overview of transparent bridging, a definition of the forwarding database (FDB) along with a summary of the FDB configuration commands.
Upon completion of this chapter, you will be able to:

- Explain different bridge types
- Define Transparent Bridging
- Explain the Extreme Networks Switch Port Status
- Describe Learning/Flooding
- Define Forwarding
- Explain Filtering
- Define the Forwarding Database – FDB
- Describe FDB CLI configuration commands
- Successfully complete the lab exercises on FDB

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

Upon completion of this chapter, you will be able to:

- **Explain different bridge types**
- **Define Transparent Bridging**
- **Explain the Extreme Switch Port Status**
- **Understand Learning/Flooding**
- **Understand Forwarding**
- **Understand Filtering**
- **Define the Forwarding Database – FDB**
- **Describe FDB CLI configuration commands**
- **Successfully complete the lab exercises on FDB**

Notes:

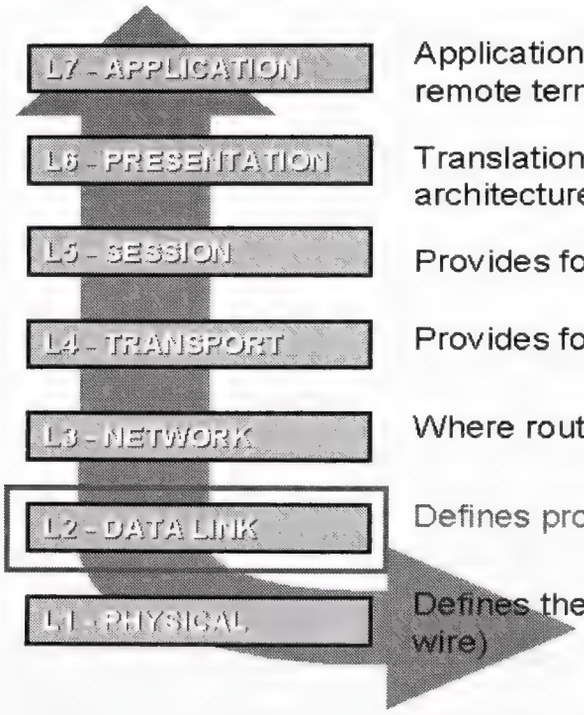
The Data Link layer defines different protocols for exchanging data frames. This layer, then, is the focus of our chapter on the subject of bridging.

The primary purpose of the Data Link layer is to provide error-free communications across a physical link.

This layer provides the basic framing and data encapsulation functions and allows for error detection.

© 2001 Extreme Networks,Inc. All rights reserved

ISO Seven Layer Reference Model



Application level access to the network, file transfer, remote terminals etc.

Translation of data structures between differing architectures

Provides for dialogue control between processes

Provides for end to end connection between machines

Where routing takes place

Defines protocols for exchanging data frames

Defines the standards for physical connections (the wire)

Notes:

Bridges Used for LAN Segmentation

Bridges were widely used to segment Ethernet collision domains with the effect of providing more bandwidth to the network user, however, they have since been replaced by switches. Bridges operate at the MAC sub-layer of layer 2 of the OSI Reference Model, and several different types have been developed to address the needs depending on the topology and the particular network requirements:

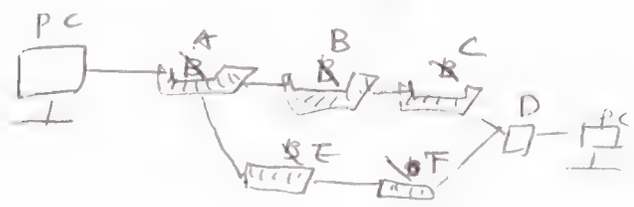
- A local bridge, which connects two or more Ethernet LAN segments
- A remote bridge, which connects Ethernet LAN via high-speed serial connection. It is accomplished with a pair of bridges using a Wide-Area Network (WAN)
- Transparent Bridging don't know how to get to Destination
- Source Route Bridging
- Source Route Transparent Bridging

Transparent Bridging
A transparent bridge makes the forwarding decisions based on the MAC destination address. This process is completely transparent to the end-devices.

Source Route Bridging
With Source Route Bridging, the source must determine the best path to get to a destination. After this path is discovered, the source station maintains the path in its source routing table and includes this path information into the Routing Information (RI) field for every packet that is sent. The Source Route Bridge is merely acting as a relay service and is looking at the RI field in every frame to make the forwarding decision. Source Routing is used in Token Ring environments (IEEE 802.5).

Source Route Transparent Bridging
This bridging method combines the two previous bridging techniques. If a frame arrives with source routing information (RI field), then the frame is source routed accordingly. If however, an RI field does not exist, then the bridge will forward the frames based on its own internal forwarding tables.

Source Route Bridging



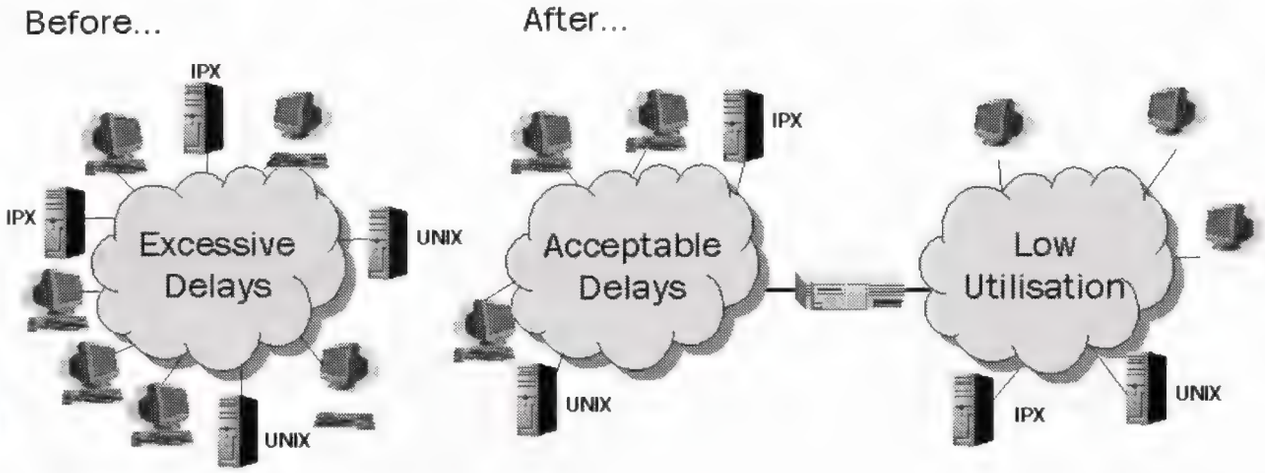
A B C D reply D C B A

A E F D reply D F E A

© 2001 Extreme Networks,Inc. All rights reserved

Bridges Used for LAN Segmentation

- **Bridges widely used to segment Ethernet collision domains**



- **Switches perform the bridge segmentation function in hardware**

Notes:

WINS
LMhost ⇒ sever1 192.168.10.1
/etc/hosts
DNS

Transparent Bridges

Transparent bridges perform segmentation of LANs by building address tables that associate segment end stations with the segment's port connection. Forwarding decisions are based on the destination MAC address inside a frame. Because bridges are L2 devices, they are L3 protocol-independent and are transparent to the end stations in an Ethernet network.

Bridges have often been referred to as "plug and play devices" because installation is easy and there is no need for further configuration because the bridge will automatically learn about the network topology. Frames are received by the bridge, in their entirety, prior to the bridge processing them. This type of bridge operation has been called "store and forward".

IEEE 802.1D is the specification for bridging, switching and spanning tree, and most of today's bridges and switches conform to this specification. One of the important roles of this standard is to specify, not only, the functions of the bridge, but also the processes that control bridge behaviour in a bridged LAN.

Because transparent bridges are unable to detect duplicate paths in a bridged LAN, an additional protocol (called the Spanning Tree Protocol) is implemented on each bridge in the LAN. The spanning tree protocol has the responsibility of detecting the topology of the network and ensuring that where duplicate paths exis they are "blocked". This process results in an "active topology" used to maintain the bridged LAN - that would otherwise suffer performance problems or constant downtime.

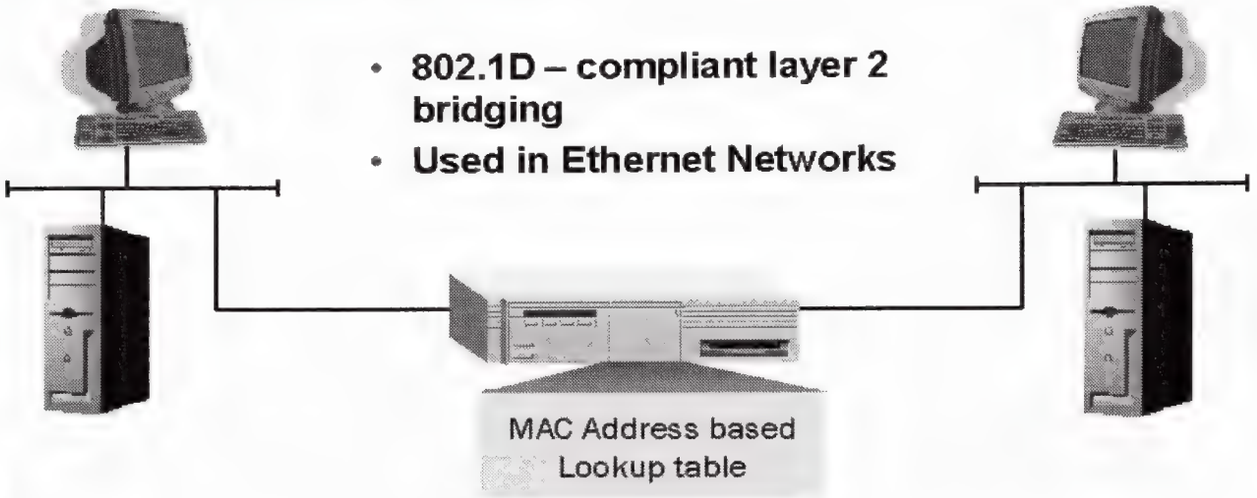
The individual bridge ports transition through various operational processes as they attempt to become part of a spanning tree "domain". The port states are discussed in this chapter, whilst spanning tree is covered in more detail in chapter 7.

In addition to the various states that a port may transition through, the bridge will carry out other necessary functions in a bridged LAN. These will include for example; flooding of frames where required, filtering of frames that do not need to be re-transmitted, and ageing out of entries in the forwarding database that have not been used recently.

All Extreme Networks switches are fully compliant, 802.1D layer-2 bridges capable of wire-speed forwarding decisions based on a given destination MAC and port pair.

© 2001 Extreme Networks,Inc. All rights reserved

Transparent Bridges



- 802.1D – compliant layer 2 bridging
- Used in Ethernet Networks

- Forwarding decisions based on destination address

Notes:

Switch Port States

The operation of an individual bridge port is described in terms of the state of the port and the operations that provide and support the functions necessary for the operation of the bridge. The state of each port controls the processing of frames received on that port and the possible inclusion of the port in the active topology of the bridged LAN.

Blocking
A port in this state does not participate in frame re-transmission, in order to prevent frame duplication caused by multiple paths existing in the active topology of the Bridged LAN. A port enters the blocking state following initialisation of the bridge, or because it has received information that another bridge is the controlling bridge for the LAN to which the port is attached (called the Designated Bridge, and covered in more detail in chapter 7). A port in blocking state can transition to the listening state or be disabled by management command.

Listening
A port in this state is "preparing" to participate in frame re-transmission, it makes no entries into the forwarding database. In the listening state, frame re-transmission is temporarily disabled in order to prevent temporary loops, which can occur as the active topology of the bridged LAN changes. A port in the listening state normally transitions to the learning state (but may transition back to the blocking state or be disabled by management command).

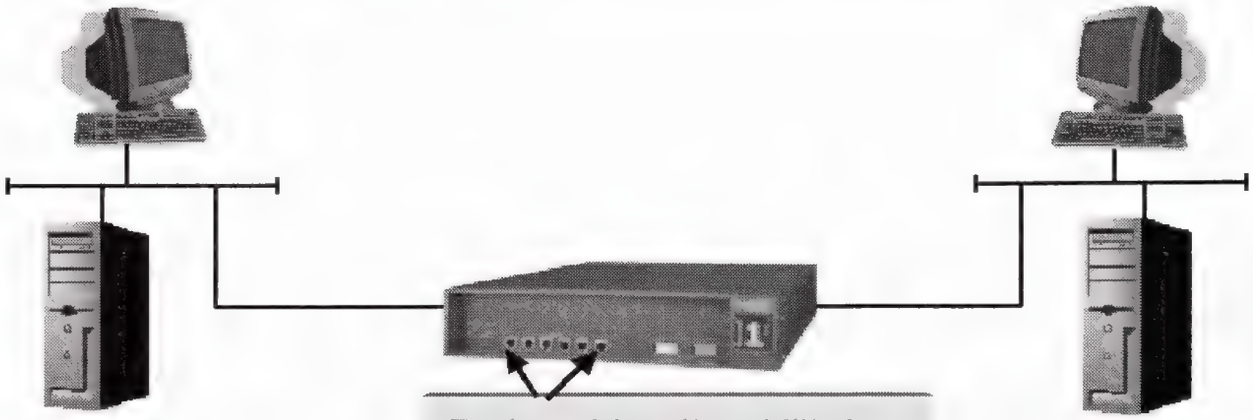
Learning
A port in this state is also "preparing" to participate in frame re-transmission. In the learning state, frame re-transmission is still temporarily disabled, however, learning is now enabled to allow information to be collected prior to frame re-transmission. The learning process examines the source addresses of frames received on each port and creates (or updates) an entry in the forwarding database associating the port on which the frame was received with the MAC Address in the source address field of the frame. A port in the learning state normally transitions to the forwarding state (but may transition back to the blocking state or be disabled by management command).

Forwarding
A port in this state is now taking part in frame re-transmission. A port in the forwarding state can forward received frames and make entries into the forwarding database. A port in the forwarding state may transition back to the blocking state or be disabled by management command.

Disabled
A port can be disabled by a management command, in which case it will not be active in the operation of the bridged LAN.

© 2001 Extreme Networks,Inc. All rights reserved

Switch Port States



Each port has the ability to:

- block
- listen
- learn
- forward
- disable

Notes:

Flooding - An Example

In this slide, and the example slides following, the operations that take place occur when the port is in the forwarding state. This slide shows an example of a newly configured network, where host "A" is attempting to communicate with host "B".

In this situation, host A transmits an initial packet to host B. The function of the bridge is to receive all packets on the networks it is connected to, and make forwarding decisions based on MAC addresses in the frames and in its own forwarding database.

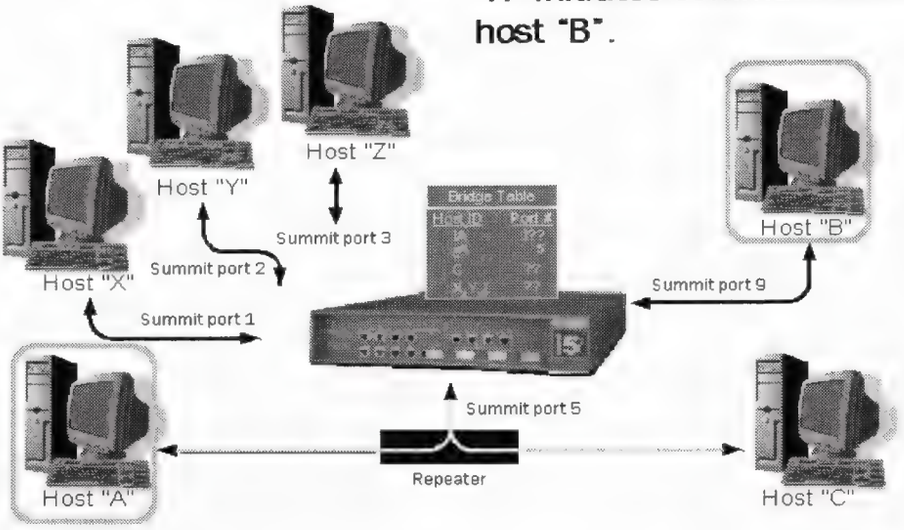
At this point in time, no MAC addresses have been learnt by the bridge and the forwarding database is empty.

Because the forwarding database is empty, the destination is considered to be unknown, and the packet must be forwarded over every attached interface in an attempt to reach all the nodes. This process, referred to as "flooding", allows host "A" to be learned on the inbound port (and an entry is added to the forwarding database).

© 2001 Extreme Networks,Inc. All rights reserved

Flooding - An Example

In a newly configured network, host "A" initiates communication with host "B".



Because the destination is unknown, the packet is flooded to all of the interfaces and host "A" is learned on the inbound port.

Notes:

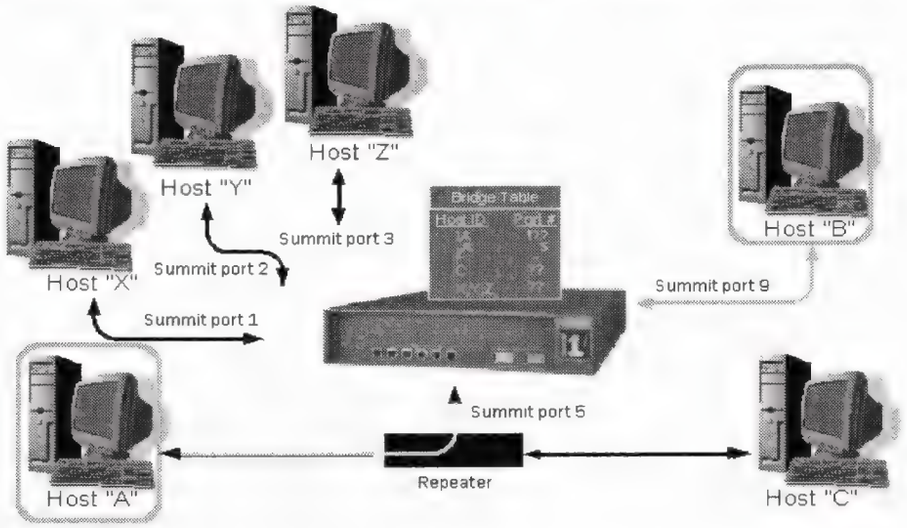
Forwarding State - An Example

In our example shown, host A transmits a frame to host B, and the bridge receives the packet:

- The bridge performs a forwarding table lookup on the destination address. If the address is known, the bridge identifies the port on which the destination address is located
- If the port is different to the port on which the frame is received, the frame is forwarded to the destination port
- If the source address does not exist in the Forwarding Database (FDB) it is added

© 2001 Extreme Networks,Inc. All rights reserved

Forwarding State - An Example



Host "B" replies to host "A", and the packet is forwarded onto the destination port learned for "A". At the same time, the MAC address for "B" is learned and added to the bridge table.

Notes:

Filtering - An Example

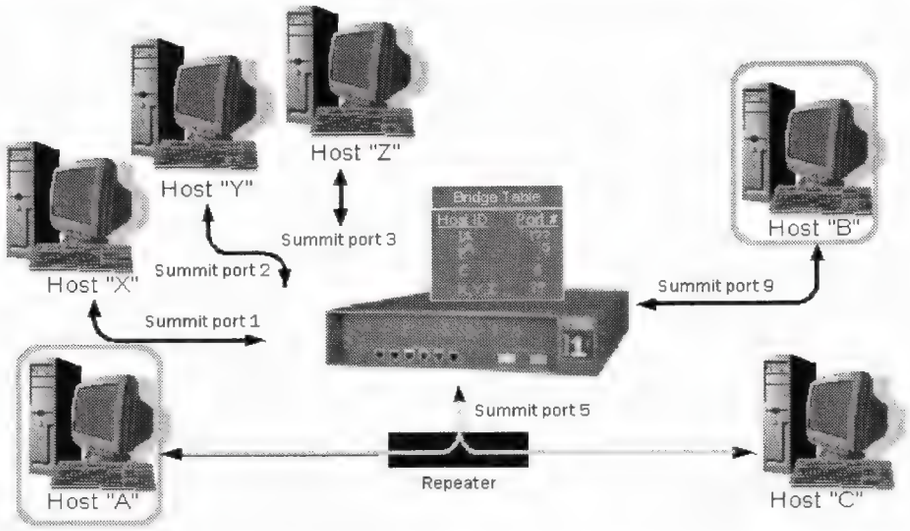
Using the same network configuration but a different operation, host A transmits a frame to host C, and the bridge receives the frame.

Both workstations are attached to the same switch port (using a simple repeater device for example purposes), and the switch learns the MAC addresses of all workstations that are active on a single port in the same way it would for a single workstation attached to a port.

When frames are received and the destination MAC address matches the inbound port, the switch drops (filters) the frame at the port. This reduces traffic on the other ports within the broadcast domain (VLAN) and optimises performance.

© 2001 Extreme Networks,Inc. All rights reserved

Filtering - An Example



When the destination MAC address matches the inbound port, the switch will drop the packet at the port. This reduces traffic on the other ports within the broadcast domain (VLAN) and optimises performance.

Notes:

ExtremeWare's Forwarding Database

The switch maintains a database of all MAC - media access control addresses received on all of its ports. The bridge table is called the Forwarding Database (FDB) and it uses the information in this database to decide whether a frame should be forwarded or filtered.

The Forwarding Database holds up to a maximum of 256,000 L2/L3 MAC entries depending on the product:

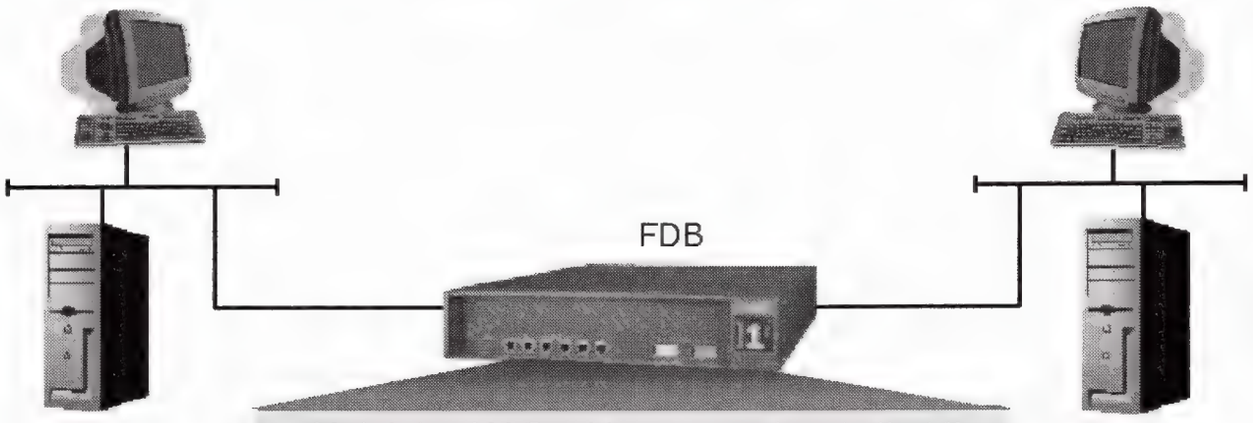
- 256,000 – BlackDiamond with all i-series modules, Summit7i, Summit 5i, and Alpines
- 128,000 – Summit1i, 48i
- 32,000 – non-i series switches

Each entry consists of the MAC address of the device, an identifier for the port on which it was received, and an identifier for the VLAN to which the device belongs. Frames destined for devices that are not in the FDB are flooded to all ports within the VLAN.

NOTE: Internally, the L2 database (FDB) and the L3 database (IPFDB) are combined in one large table.

© 2001 Extreme Networks,Inc. All rights reserved

ExtremeWare's Forwarding Database



- Maintains MAC addresses and ports that they were learned on
- Up to 256,000 L2/L3 MAC entries
- Each entry consists of:
  - MAC address
  - Port ID
  - VLAN ID

Notes:

FDB Entry Types

Possible flag values in a FDB display are:

Dynamic Entries
Initially, all entries in the database are dynamic. Entries in the database are removed (or "aged-out") if, after a period of time (the "aging time"), the device has not transmitted. This prevents the database from becoming full with obsolete entries by ensuring that when a device is removed from the network, its entry is deleted from the database. Dynamic entries are deleted from the database if the switch is reset or a power off/on cycle occurs.

Non-aging Entries
If the aging time is set to zero, all aging entries in the database are defined as static, non-aging entries. This means that they do not age, but they are still deleted if the switch is reset.

Permanent Entries
Permanent entries are retained in the database if the switch is reset or a power off/on cycle occurs. The system administrator must make entries permanent. A permanent entry can either be a unicast or multicast MAC address. All entries entered by way of the command-line interface are stored as permanent.

- The Summit switch supports a maximum of 64 permanent entries
- The Summit7i and Alpine 3803 supports a maximum of 256 permanent entries
- The BlackDiamond switch supports a maximum of 512 permanent entries (EW6.1+)

Once created, permanent entries stay the same as when they were created. For example, the permanent entry store is *not* updated when any of the following take place:

- A VLAN is deleted
- A VLANid is changed
- A port mode is changed (tagged/untagged)
- A port is deleted from a VLAN
- A port is disabled
- A port enters blocking state
- A port QoS setting is changed
- A port goes down (link down)

Blackhole Entries
A blackhole entry configures the switch to discard packets with a specified MAC destination address. Blackhole entries are useful as a security measure or in special circumstances where a specific destination address must be discarded. Blackhole entries are treated like permanent entries in the event of a switch reset or power off/on cycle. Blackhole entries are never aged out of the database.

© 2001 Extreme Networks,Inc. All rights reserved

FDB Entry Types

- **Dynamic entries**
  - Initially, all entries in the database are dynamic
- **Static entries**
  - Non-aging entries
    - Entries whose aging time is set to zero
  - Permanent entries
    - Entered via the CLI are stored as permanent
    - Retained in the database even on reset/power off
    - Max. 256 for Summit7i & Alpine, 512 for BlackDiamond
  - Blackhole entries
    - Configures packets with specified MAC destination address to be discarded.

Notes:

Create FDB Entry

Entries are added into the FDB in the following ways:

- The switch can learn entries dynamically. The system updates its FDB with the source MAC address from a packet, the VLAN, and the port identifier on which the source packet is received
- You can enter and update entries using an SNMP Network Manager, or the command-line interface CLI

CLI Command - create fdbentry
create fdbentry <mac_addr> vlan <name> [blackhole | dynamic | port [all | <port number>]]
Creates a permanent FDB table entry for a specified MAC address..

CLI Command - delete fdbentry
delete fdbentry <mac_address> vlan <vlan name>
Deletes an FDB entry.

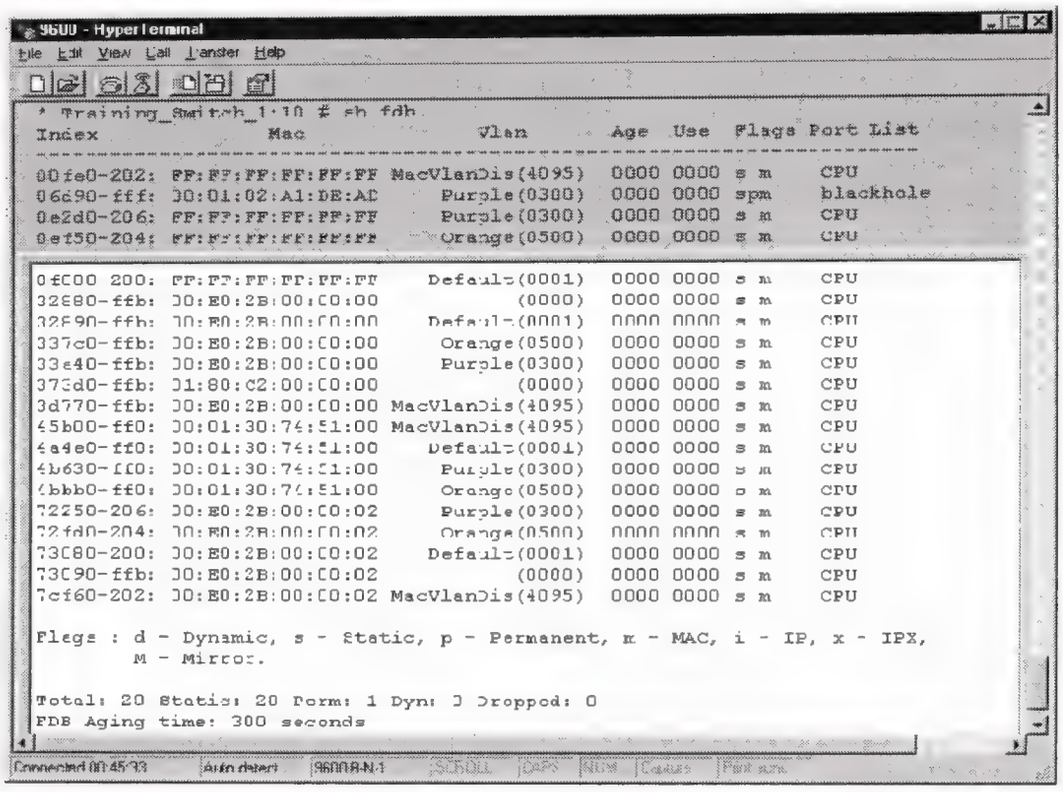
CLI Command – FDB aging time
config fdb agingtime <seconds>
This configures the FDB aging time from 15-1,000,000 seconds. The default is 300 seconds. A value of 0 indicates that the entry should never be aged out.

CLI Command - clear fdb
clear fdb {ports <port number> | vlan <vlan name> | <hex octet> }
Clears dynamic FDB entries matching the filter. When no options are specified, the command clears all dynamic entries.

CLI Command – show fdb
show fdb {permanent | ports <port number> | vlan <vlan name> | <hex octet>}
Displays the FDB table entries that match the filter. When no options are specified, the command displays all FDB entries.

© 2001 Extreme Networks,Inc. All rights reserved

Create FDB Entry


9600 - HyperTerminal
File Edit View Call Transfer Help
* Training_Switch_1:10 # sh fdb
Index Mac Vlan Age Use Flags Port List
00fe0-202: FF:FF:FF:FF:FF:FF MacVlanDis(4095) 0000 0000 s m CPU
06c90-fff: 00:01:02:A1:DE:AD Purple(0300) 0000 0000 spm blackhole
0e2d0-206: FF:FF:FF:FF:FF:FF Purple(0300) 0000 0000 s m CPU
0ef50-204: FF:FF:FF:FF:FF:FF Orange(0500) 0000 0000 s m CPU
0fC00 200: FF:FF:FF:FF:FF:FF Default(0001) 0000 0000 s m CPU
32e80-ffb: 00:E0:2B:00:C0:00 (0000) 0000 0000 s m CPU
32f90-ffb: 00:E0:2B:00:C0:00 Default(0001) 0000 0000 s m CPU
337c0-ffb: 00:E0:2B:00:C0:00 Orange(0500) 0000 0000 s m CPU
33e40-ffb: 00:E0:2B:00:C0:00 Purple(0300) 0000 0000 s m CPU
373d0-ffb: 01:80:C2:00:C0:00 (0000) 0000 0000 s m CPU
3d770-ffb: 00:E0:2B:00:C0:00 MacVlanDis(4095) 0000 0000 s m CPU
45b00-ff0: 00:01:30:74:51:00 MacVlanDis(4095) 0000 0000 s m CPU
4a4e0-ff0: 00:01:30:74:51:00 Default(0001) 0000 0000 s m CPU
4b630-ff0: 00:01:30:74:51:00 Purple(0300) 0000 0000 s m CPU
4bbb0-ff0: 00:01:30:74:51:00 Orange(0500) 0000 0000 s m CPU
72250-206: 00:E0:2B:00:C0:02 Purple(0300) 0000 0000 s m CPU
72fd0-204: 00:E0:2B:00:C0:02 Orange(0500) 0000 0000 s m CPU
73C80-200: 00:E0:2B:00:C0:02 Default(0001) 0000 0000 s m CPU
73C90-ffb: 00:E0:2B:00:C0:02 (0000) 0000 0000 s m CPU
7cf60-202: 00:E0:2B:00:C0:02 MacVlanDis(4095) 0000 0000 s m CPU
Flags : d - Dynamic, s - Static, p - Permanent, m - MAC, i - IP, x - IPX,
M - Mirror.
Total: 20 Static: 20 Perm: 1 Dyn: 0 Dropped: 0
FDB Aging time: 300 seconds

Notes:

00-01-30 for extreme company

Summary

Chapter five has taken you through the description of different bridge types used in segmenting LANs, the various functions a bridge performs, and how the bridge handles frames received from the networks it is attached to. You should now be able to:

- Explain the different bridge types
- Define Transparent Bridging
- Explain the Extreme Networks Switch Port Status
- Describe Learning/Flooding
- Define Forwarding
- Explain Filtering
- Define the Forwarding Database – FDB
- Describe FDB CLI configuration commands
- Successfully complete the lab exercises on FDB

© 2001 Extreme Networks,Inc. All rights reserved

Summary

You should now be able to:

- **Explain different bridge types**
- **Define Transparent Bridging**
- **Explain the Extreme Switch Port Status**
- **Describe Learning/Flooding**
- **Describe Forwarding**
- **Describe Filtering**
- **Define the Forwarding Database – FDB**
- **Describe FDB CLI configuration commands**
- **Successfully complete the lab exercises on FDB**

Notes:

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 6

VLAN and Port Configuration

Chapter Objectives

Chapter six examines the different types of Virtual Local Area Networks (VLANs) that can be configured in the Extreme Networks switch family.

Upon completion of this chapter, you will be able to:

- Define VLANs at an overview level
- Describe VLANs in Extreme Networks Switches
- Distinguish between VLAN types:
- port-based
- tagged
- MAC-based
- protocol-based
- vMANs
- Configure:
- Port-based VLANs
- VLAN tagging
- MAC-based VLANs
- Define Protocol-based VLANs
- Explain vMANs
- Successfully complete the lab exercises

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

Upon completion of this chapter, you will be able to:

- **Define VLAN in an overview**
- **Describe VLAN in Extreme Networks Switches**
- **Distinguish between VLAN types-port-based, tagged, MAC-based, protocol-based, and vMANs**
- **Configure**
  - Port-based VLAN
  - VLAN tagging on an Extreme Networks Switch
  - MAC-based VLAN
- **Define protocol-based VLANs**
- **Explain vMAN and Jumbo Frames**
- **Successfully complete the lab exercises**

Notes:

What are VLANs?

Virtual LANs (VLANS) are a technology that provides the network administrator with greater control over network traffic and administration.

- A VLAN is a Layer 2 broadcast domain
- With the use of VLANs the Layer 2 broadcast domain a device is a member of, is no longer defined by just its physical location
- VLANs allow the administrator to define which devices are contained within the same Layer 2 broadcast domain
- Devices configured to be within the same VLAN communicate as though they were on the same physical network (regardless of physical location)

VLANs greatly increase the control available to the administrator. VLANs can enhance network performance and design flexibility as:

- A single switch may be configured to support multiple VLANs.
- A single port on a switch can be a member of more than one VLAN.
- A single VLAN can span multiple switches.

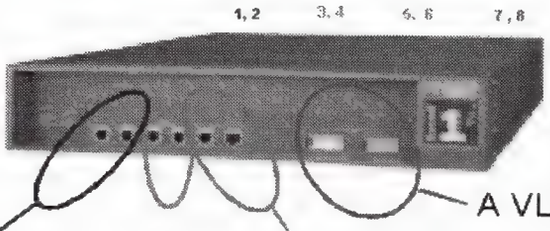
Devices configured in different VLANs cannot communicate at Layer 2. Network traffic needs to be routed between these VLANs. This means that VLANs need to be configured with an IP address if you wish to communicate (i.e. route) between them

On Extreme Networks Switches at least one VLAN must be configured with an IP address if you want to manage the VLANs on that switch. Setting up VLANs on the switch eases many time-consuming tasks of network administration while increasing efficiency in network operations.

© 2001 Extreme Networks,Inc. All rights reserved

What are VLANs?

- **A virtual Local Area network is a collection of devices that communicate as if they were on the same broadcast domain**



A VLAN is a logical interface

Each VLAN is an independent broadcast domain

One or more switch ports as members

- **VLAN configuration and operation is integral to the overall function of the Extreme Switch**

Notes:

VLAN Benefits

Implementing VLANs on your networks offers several advantages:

VLANS help to control traffic:
VLANs provide a way of defining the size of Layer 2 broadcast domains and which devices are members of the domain. This is important to network design as controlling Layer 2 broadcasts is a factor in overall network performance. The important issue is that this domain is not controlled by physical location. If required, each port of the same switch could be configured to a different VLAN.

VLANS provide extra security
Devices within each VLAN can only communicate (at Layer 2) with member devices in the same VLAN. If a device in VLAN *Marketing* must communicate with devices in VLAN *Finance*, the traffic must cross a routing device.

NOTE:
If you wish to monitor the traffic on the network by using a "Sniffer" type of device, you will only see the Layer 2 information for the VLAN (broadcast domain) you are connected to.

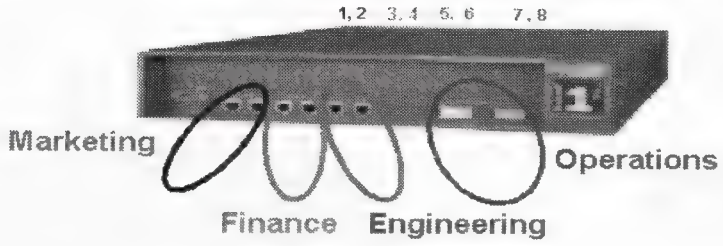
VLANs ease the change and movement of devices
With traditional networks, network administrators spend much of their time dealing with moves and changes. If users who were configured to be in a specific Layer 2 broadcast domain physically move location, it can be difficult (or impossible) to reconfigure the network to maintain them as members of the same broadcast domain.

By implementing VLANs, if an end-station in VLAN *Marketing* is moved to a port in another part of the network and needs to retain its original VLAN membership, you only have to specify that the new port is a member of VLAN *Marketing*. There is no need to physically reconfigure the network

© 2001 Extreme Networks,Inc. All rights reserved

VLAN Benefits

- **Help to control traffic**
- **Provide extra security**
  - Only devices belonging to the same VLAN will see each other's traffic.
- **Ease the change and movement of devices**



Notes:

VLAN in Extreme Network Switches

Each Summit *i*-series or Alpine switch can have a maximum of 3000 VLANs. Two of these are pre-configured on all switches:

- Default VLAN and
- MacVlanDiscover VLAN

These VLANs are discussed later.

Summit 5i, Summit7i and Alpines have an additional VLAN pre-configured called Mgmt. This VLAN is available on a specific physical port that is typically used for management functions.

Each BlackDiamond Switch has the ability to support both non *i*-series and *i*-series blades. In a switch that is configured solely with *i*-series a maximum of 3000 VLANs can be configured.

VLANs are identified by unique names. If you wish to create a VLAN you use the following command:

CLI Command – create VLAN
create vlan <vlan name><cr>

If a VLAN already exists you can change its name by using the command:

CLI Command – rename existing VLAN
config vlan <old_name> name <new_name>

Default VLAN

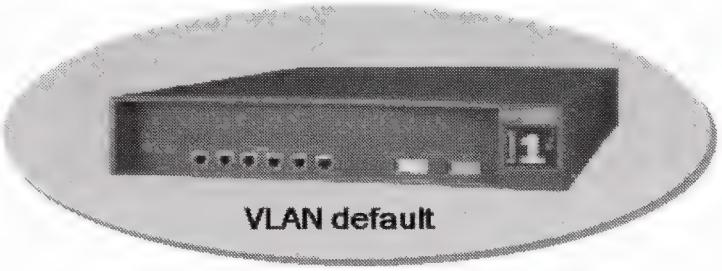
All switches ship with several pre-configured VLANs, with the VLAN "default" having the following properties:

- Has an internal VLAN id of 1
- Contains all the switch ports as members. The ports are defined as untagged, this is discussed later

NOTE: The VLAN "default" cannot be deleted. Although you can rename an existing VLAN, the "default" and "MacVlanDiscover" VLAN names should not be changed. VLAN names are not case sensitive.

© 2001 Extreme Networks,Inc. All rights reserved

VLAN in Extreme Networks Switches



VLAN default

- Comes pre-configured on all switches
- All ports are members
- Internal VLAN id of '1'

- **Maximum of 3000 VLANs in *i*-series or Alpine Switch**
- **Each BlackDiamond can have a maximum of 3000 VLANs in all *i* -series systems**
- **Each VLAN has a unique name**

Notes:

rename VLAN won't get back to original Default.

VLAN - MacVlanDiscover

All Extreme Networks i-series switches come pre-configured with a VLAN called MacVlanDiscover, which has the following features:

- It is a MAC-based VLAN (discussed later)
- It has no member switch ports
- It has an internal VLAN id of 4095 (ids are discussed later)
- It cannot be deleted*

* Although you can change the name, the original name is recreated after a reboot.

© 2001 Extreme Networks,Inc. All rights reserved

VLAN - MacVlanDiscover

- A pre-configured MAC-based VLAN
- Found only on all *i*-series switches
- No member switch ports
- Has an internal VLAN id of "4095"
- Cannot be deleted
- Although you can change the name, the original name is recreated after the reboot
- *More on this later*

Notes:

Types of VLANs

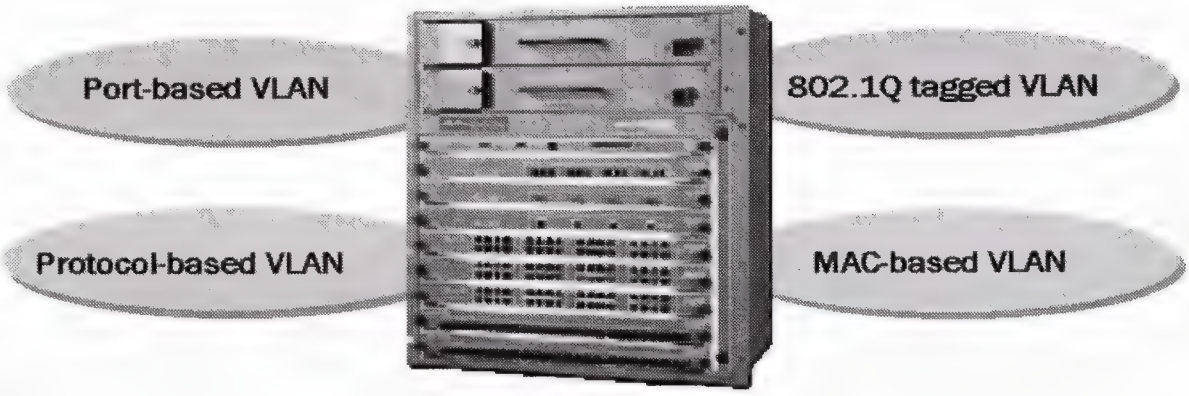
VLANs can be created on the Extreme Networks switch according to the following criteria:

- Port-based (Untagged) VLAN
- 802.1Q Tagged VLAN
- MAC-based VLAN (MAC address)
- Protocol-based VLAN
- Ethernet, LLC SAP, or LLC/SNAP Ethernet protocol type
- Treated like a Tagged VLAN
- A combination of any of the above

Each of these VLAN types is discussed in the following slides.

© 2001 Extreme Networks,Inc. All rights reserved

Types of VLANs



- Or a combination of the above

Notes:

Port-Based VLANs

In a port-based VLAN, a VLAN is configured to a group of one or more ports on the switch. A port can be a member of only one port-based VLAN.

- A port-based VLAN is also known as an "untagged" VLAN

For the members of different VLANs to communicate, the switch must route the traffic, even if they are physically part of the same I/O module. This means that each VLAN must be configured as a router interface with a unique IP address.

To create VLANs that span two (or more) switches in a port-based VLAN, the switches must be connected together by a cable that connects ports on each switch that have been configured with the same VLAN name

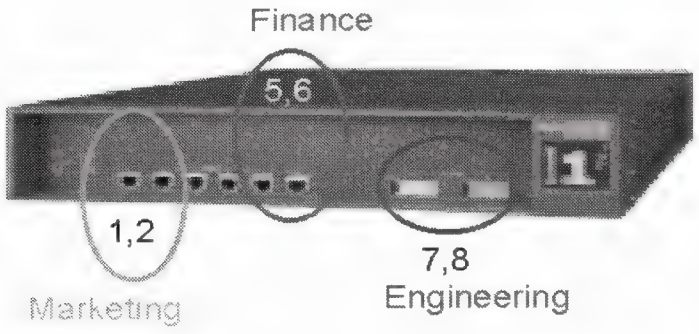
Using this configuration, you can create multiple VLANs that span multiple switches, in a daisy-chained fashion.

- Each switch must have a configured port(s) for each VLAN. Each link between the switches ports must connect to a port that is a member of the same VLAN on the next switch.

untagged port can run only one VLAN.
(no two ports-based VLAN in Extreme)
Some vendors allow you to do this

© 2001 Extreme Networks,Inc. All rights reserved

Port-Based VLANs



- **Also known as "untagged" VLANs**
- **Port members are untagged**
- ***A port can only be a member of one port-based VLAN***

Notes:

Configuring Port-based VLANs

Because a port can only be a member of one port-based VLAN, the error detailed in the slide is often seen when you are first gaining experience of configuring port based VLANS.

The error indicates that port 1 is already a member of a port-based VLAN other than **test**. To solve this you can do one of the following:

- remove port 1 from the original port-based VLAN
- make VLAN **test** a tagged VLAN and add port 1 tagged (tagging is discussed later)
- make VLAN **test** a protocol-based VLAN (protocol based VLANs are discussed later)

Important Note:
Problem: Because VLAN Default initially contains all the switch ports as members (port based i.e. untagged), this error will always appear each time you create and configure a port-based VLAN and add a port untagged.

Solution: Delete all ports on VLAN Default before attempting to create and configure new port-based VLANs.

CLI Command – delete default ports
config default delete ports all
Deletes all ports from the pre-configured VLAN Default.

CLI Command – create port-based VLAN
create vlan <vlan_name>
Creates a port-based VLAN, an example might be – create vlan blue.

CLI Command – add ports to VLAN
config <vlan_name> add ports [all | <port number>]
Configures a VLAN by adding all ports, or a specified range of ports. An example might be - config blue add port 1,2.

© 2001 Extreme Networks,Inc. All rights reserved

Configuring Port-based VLANs

- **When configuring a VLAN, you get an error:**
  Summit1iTx:17 # config vlan test add port 1
  ERROR: There is a protocol conflict with adding port 1 untagged to vlan "test". Either add this port as tagged or assign another protocol to this vlan

- **And upon examining existing VLANs, we find this:**

```
* Summit1iTx:18 # sh vlan default
VLAN Interface[0-200] with name "Default" created by user
Tagging:      802.1Q Tag 1
IP:           Waiting for bootp reply.
STPD:         Domain "s0" is not running spanning tree protocol
Protocol:     Match all unfiltered protocols.
Loopback:     Disable
Rate Shape:   Disable
QosProfile:   QP1
Ports:        8.   (Number of active ports=0)
Untag:        1 2 3 4 5 6 7 8
```

Notes:

Inter-VLAN Communication - Single Switch

A single switch is shown with four IP VLANs with ports created and configured. When the IP VLANs are required to communicate with each other, the switch must route the traffic, even though they are physically part of the same switch or switch I/O module.

The routing software and hardware routes IP traffic between router interfaces. A router interface is a VLAN that has an IP address assigned to it.

To assign an IP address to a VLAN you use the following command:

CLI Command – configure VLAN IP address
configure <vlan_name> ipaddress <ip_address>/<netmask>
Configures a VLAN with IP address, an example might be:
- config blue ipaddress 10.10.1.1/24

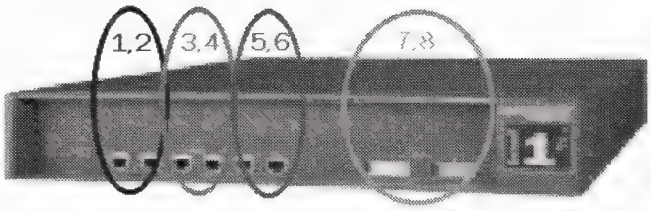
CLI Command – show iproute
show iproute
Allows you to verify new routes.

NOTE: The VLANs must have IP forwarding enabled (this is a per VLAN function). If you use the CLI command "enable ipforwarding" (ie. not specifying a particular VLAN), IP forwarding will be enabled on all currently configured VLANs.

© 2001 Extreme Networks,Inc. All rights reserved

Inter-VLAN Communication

Single Switch



- Traffic must be routed by the switch even if the VLANs are physically part of the same device
- The routing software and hardware routes IP and IPX traffic between router interfaces. A router interface is a VLAN that has an IP address assigned to it

Notes:

Port-based VLANs - Steps for Spanning Switches

The slide shows three VLANs configured across two switches. The following steps show the basic process involved in configuring each of the three VLANs:

- Create the VLANs on each switch

- Create vlan finance
- Create vlan engineering
- Create vlan marketing

- Configure to add port/s on each VLAN per switch

- Config finance add ports 1-2
- Config engineering add ports 5-6
- Config marketing add ports 7-8

- Configure ipaddress on each of the VLANs for inter-VLAN communications

- Config finance ipaddress x.x.x.x/x
- Config engineering ipaddress x.x.x.x/x
- Config marketing ipaddress x.x.x.x/x

- Physical VLAN connectivity is achieved by cabling the switches together using one port on each switch per VLAN

This type of physical connection is wasteful of physical port resources, and is overcome with the implementation of other VLAN types such as VLAN tagging.

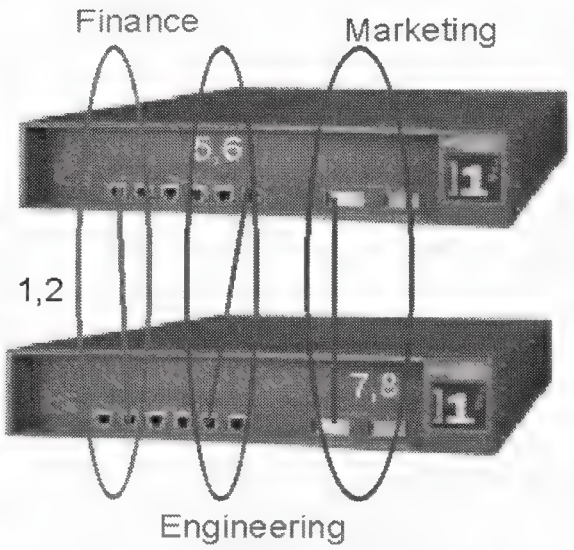
NOTE: Port-based VLANs are also known as untagged VLANs

© 2001 Extreme Networks,Inc. All rights reserved

Port-based VLANs

Steps for Spanning Switches

- **Physically cable switches together using one port on each switch per VLAN, then:**
  - Create VLANs per switch
  - Configure to add port/s on each VLAN per switch
  - Configure IP address on each of the VLANs for inter-VLAN communications



Finance to Finance
→ don't need IP address

Finance to ~~Finance~~ Engineering
→ need ip

Notes:

Introducing VLAN Tagging

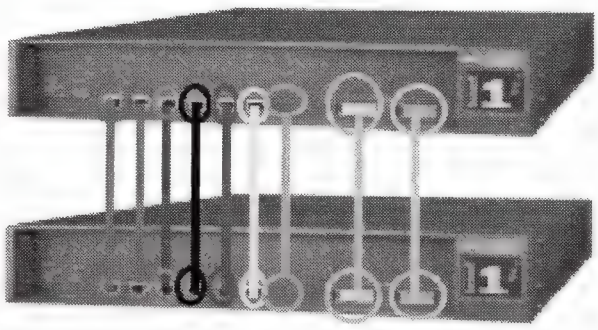
In the example shown on the slide, let us assume that we are using Port based VLANs, and that all 8 ports of the top switch are already connected to all eight ports of the lower switch for 8 different VLANs. When a ninth VLAN is required there are no more ports to use!

The introduction of a different VLAN technique called VLAN tagging solves the problem of having to use multiple ports (if you have multiple VLANs) for inter-VLAN communications.

© 2001 Extreme Networks,Inc. All rights reserved

Introducing VLAN Tagging

- **When spanning multiple switches**
  - What if you have more VLANs to configure and no more physical ports to connect between switches?



Notes:

VLAN Tagging Overview

VLAN "tagging" is a process that inserts a marker (called a tag) into the Ethernet frame. The tag contains the identification number of a specific VLAN, called the VLAN id.

Tagging is most commonly used to create VLANs that span switches. The switch-to-switch connections are typically called *trunks*. Using tags, multiple VLANs can span multiple switches using just one trunk. It is also possible (and common) to use multiple trunks.

VLAN Tagging is an integral function to the operation of all Extreme Networks switches and their ability to support VLANs.

The IEEE 802.1Q VLAN specification defines the Ethernet Tagging specification. This is currently the only standard (i.e. non proprietary) for this technology.

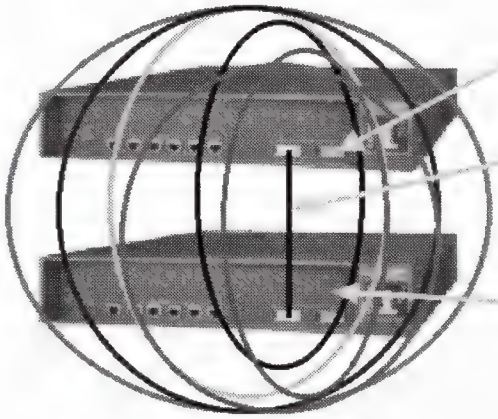
Another benefit of tagged VLANs is the ability to have a port configured as a member of multiple VLANs. This is particularly useful if you have a device (such as a server) that must belong to multiple VLANs. The device must have a Network Interface Card (NIC) that supports IEEE 802.1Q tagging.

As a single port can only be a member of one port-based VLAN, tags must be used for all additional VLAN membership for that port.

NOTE: The use of 802.1Q tagged packets may lead to the appearance of packets slightly bigger than the current IEEE 802.3/Ethernet maximum of 1,518 bytes. This may affect packet error counters in other devices, and may also lead to connectivity problems if non-802.1Q bridges or routers are placed in the path. (The current version of IEEE 802.1D specifies that a device can receive up to 1,522 bytes).

© 2001 Extreme Networks,Inc. All rights reserved

VLAN Tagging Overview



- **IEEE 802.1Q VLAN specification**
- **Allows a single connection between switches to carry traffic for multiple VLANs**
- **A process that inserts a marker (called a tag) into the Ethernet frame**
  - Contains a unique number of the VLAN, called the VLAN id

Notes:

VLAN Tagging - Dependencies

When a switch receives a frame from a port, the switch has to find out if the frame was carrying a tag. Conversely, when the switch has to send a frame out to a port the switch has to decide if the frame needs to carry a tag on the outgoing direction.

In other words, the switch has to know if a port is configured as a tagged or an untagged port.

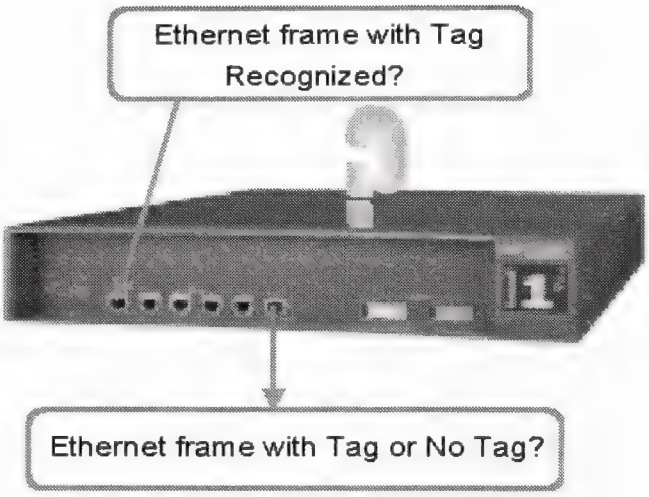
Tagging has two methods of operation:

- Implicit tagging is used in association to a given port, which has an implicit tag value that has been assigned by the switch
- Explicit tagging is defined by the reception of an already tagged frame. It explicitly defines itself by having an already populated tag within the MAC header. This tag is what the user/administrator configures

NOTE: ExtremeWare will drop an explicitly tagged frame that does not match the defined values for a given port.

© 2001 Extreme Networks,Inc. All rights reserved

VLAN Tagging - Dependencies



- **Implicit Tagging**
  - **Packets without 802.1Q tags**
  - **Only one implicit tag per port**
  - **Applies to Port-based VLANs**
- **Explicit Tagging**
  - **Packets with 802.1Q tags**
  - **Multiple explicit tags per port**
  - **Applies to Tagged VLANs**

10, 20, 30 on port 1

40 get into port 1

→ Explicit Tagging

→ will be out

Notes:

Ethernet Frame - Before and After Tagging

The diagram shows the Ethernet frame before and after the addition of the 802.1Q fields. See the information detailed below for an explanation of the fields shown.

Tag Protocol Identifier (TPI) field

- This has a value outside the possible range of Ethernet Type or Length entries, allowing identification of the field as a Tag Protocol Identifier
- Can be either Ethernet-encoded or SNAP-encoded for token ring or FDDI:
    - If Ethernet encoded, the field contains these four hex digits: 81 00
    - If SNAP encoded, the field begins with hex digits AA-AA-03 and is 8 octets long instead of 2 octets

Tag (TAG) portion

- User Priority field:
    - 3 bits (priorities 0-7) available
    - A higher number means a higher priority

7- priority (high)

- Canonical Format Indicator (CFI) field:
    - Specifies order of significant bits within the data field
    - A CFI setting of 1 in a tagged Ethernet frame is used when a token ring or FDDI frame is encapsulated within the Ethernet frame
- VLAN Identifier field:
    - 4096 possible values
    - 0 entry "Null VLAN ID", which is used for STP bridge PDUs, for example. The frame is handled like an untagged frame, with the possibility of an 802.1p priority setting.
    - VLAN ID 4095 is reserved

© 2001 Extreme Networks,Inc. All rights reserved

Ethernet Frame –
Before & After Tagging

Normal Ethernet Frame

Preamble: 7	SFD: 1	DA: 6	SA: 6	Type/ Length: 2	Data: 46 to 1500	CRC: 4

inserted fields

IEEE 802.1Q Tagged Frame

Preamble: 7	SFD: 1	DA: 6	SA: 6	2 TPI	2 TAG	Type/ Length: 2	Data: 46 to 1500	CRC: 4

User Priority	CFI	Bits of VLAN ID to identify 4,096 possible VLANs
3 bits	1 bit	12 bits

Notes:

Tagged VLANs on Extreme Networks Switches

As previously discussed, tagging is most commonly used to create VLANs that span switches using trunks.

The diagram shows the situation before tagging, which requires all VLANs spanning the switches to have a physical connection (port based VLANs), and the situation after tagging, with only one physical connection spanning multiple VLANs with tags.

Each VLAN configured in the switch may be assigned an 802.1Q VLAN tag. As ports are added to a VLAN with an 802.1Q tag defined, you decide whether each port will use tagging for that VLAN.

CLI Command – VLAN tag value
Config vlan <vlan_name> tag <tag value>
Configures the VLAN with a tag value, an example might be:
- config default tag 40

CLI Command – add port tagged
Config vlan <vlan_name> add port [all | <port number>] tagged
Configures a port to use tags for a given VLAN.

The default mode of the switch is to have all ports assigned untagged to the VLAN named "default" with an 802.1Q VLAN tag (VLAN id) of 1 assigned.

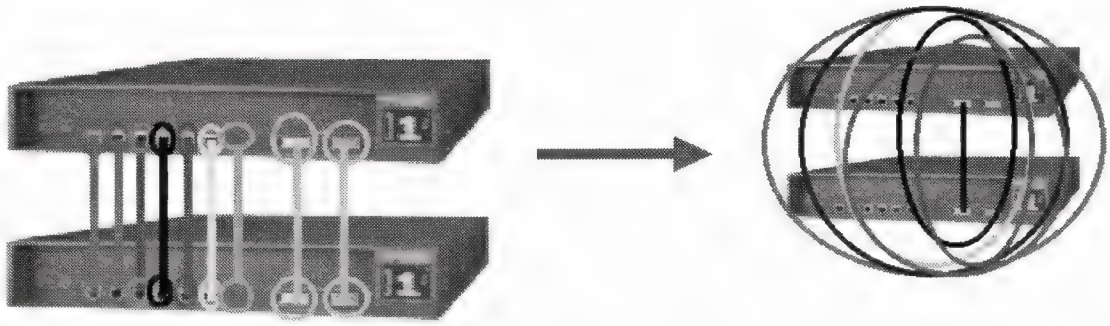
Not all ports in the VLAN must be tagged. As traffic from a port is forwarded out of the switch, the switch determines (in real time) if each destination port should use tagged or untagged frame formats for that VLAN. The switch adds and strips tags, as required, by the port configuration for that VLAN.

NOTE: Packets arriving tagged with a VLAN id that is not configured on the switch will be discarded.

NOTE: Keep in mind that end stations may not recognise tagged frames coming from the switch port it is connected to. These end workstations will discard this frame because where the expected a Type/Length field, there is a tag value inserted into it.

© 2001 Extreme Networks,Inc. All rights reserved

Tagged VLANs on Extreme Networks Switches



- **Provides for VLANs to span 2 or more switches**
  - With only a single interconnection between switches
- **A port can be a member of multiple VLANs**
  - Only one of the VLANs it belongs to can be a port-based VLAN
  - The rest of the VLANs should be either tagged, protocol-based or MAC-based.

Notes:

Configuring Tagged VLANs

Listed below are the steps that will enable you to configure VLANs with tags and then configure the VLAN with ports that are tagged:

CLI Command – create VLAN
create vlan <vlan_name>
Creates a VLAN with a unique name.

CLI Command – VLAN IP address
config vlan <vlan_name> ipaddress <ip-address>/<netmask>
Configures an IP address for the VLAN (if required). Each IP address and mask assigned to a VLAN must represent a unique IP subnet. You cannot configure the same IP subnet on different VLANs.

CLI Command – VLAN tag value
config vlan <vlan_name> tag <tag value>
Configures the VLAN with a tag value (between the range of 2 - 4094).

CLI Command – VLAN tagged member ports
config <vlan_name> add ports [all | <port number>] tagged
Configures VLAN with member ports as tagged.

CLI Command – show VLAN
show <vlan_name>
Verifies that the ports are now tagged ports.

© 2001 Extreme Networks,Inc. All rights reserved

Configuring Tagged VLANs

- **First you create a VLAN**
  - create vlan test
- **Configure an ip address for the VLAN (if required)**
  - config test ipaddress 10.10.10 1/24
- **Configure the VLAN with a tag value (2 - 4094)**
  - config test tag 100
- **Configure VLAN with member ports as tagged**
  - config test add ports 1-2 tagged
  - config test add ports 3-4 untagged
- **Verify that the ports are now tagged ports**
  - show <vlan_name>

Notes:

Verify Example - show VLAN test

The slide shows the output from the CLI command – show vlan test.

After all VLAN configuration commands have been entered, it is good practice to verify the switch settings against using this command.

© 2001 Extreme Networks,Inc. All rights reserved

Verify Example – show VLAN test

```
* Summit1iTx:20 # show test
VLAN Interface[2-204] with name "test" created by user
    Tagging:                 802.1Q Tag 100
    IP:                      10.10.10.1/255.255.255.0
    STPD:                    Domain "s0" is not running spanning tree
      protocol
    Protocol:                Match all unfiltered protocols.
    Loopback:                Disable
    Rate Shape:              Disable
    QosProfile:QP1
    Ports:                   4.    (Number of active ports=0)
          Untag:             3  4
          Tagged: 1 2
* Summit1iTx:21 #
```

Notes:

More on Tagging

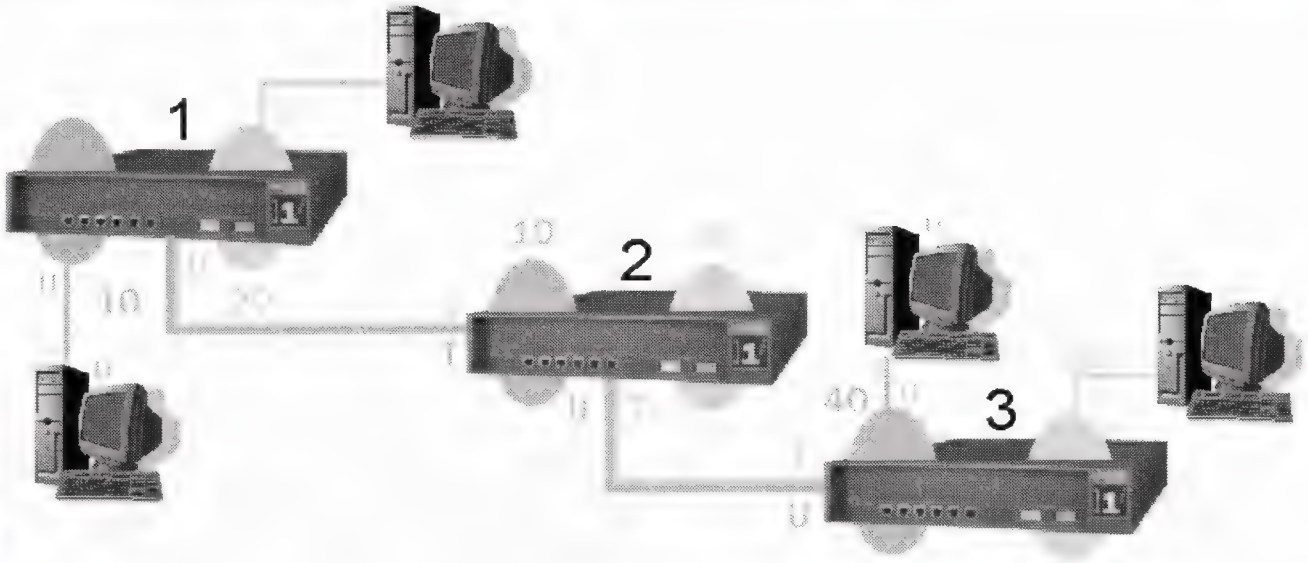
When configuring VLANs with tagging, the following points should be remembered:

- Multiple VLANs using a single, physical uplink require tags to differentiate the broadcast domains
- Tags must match across an uplink for the associated VLANs to be contiguous
- If the tags are mismatched, datagrams will be discarded at the port and the VLANs will remain partitioned

You should now be in a position to answer the question on the slide.

© 2001 Extreme Networks,Inc. All rights reserved

More on Tagging



- **If the tag values are inconsistent end-to-end, but the port tag memberships are consistent across a link, will the network exhibit continuity across the VLANs?**

Notes:

MAC-based VLANs

MAC-based VLANs allow you to designate a set of ports that have their VLAN membership dynamically determined by the MAC address of the end stations that plug into the physical port.

Dynamic determination of VLAN membership has many advantages, for example:

- This feature could be used for a roaming user who wishes to connect to their VLAN from different locations. The user might belong to the VLAN called accounting. In each location, the user can plug into one of the designated ports on the switch and is automatically mapped to the accounting VLAN
- All the benefits of being in the accounting VLAN, in terms of Quality of Service (QoS), routing, and protocol support, are maintained

When using the MAC-to-VLAN mapping, the following guidelines should be remembered:

- A port can only accept connections from an endstation/host and should not be connected to a L2 repeater/hub device. If a hub is connected and the configured MAC-to-VLAN mapped station enters the hub, any endstation that is attached to the hub can be mapped to that VLAN while the configured statio is active
- Groups are used as a security measure to allow a MAC address to enter into a VLAN only when the group mapping matches the port mapping. The group "any" is equivalent to group "0". Ports configured as "any" allow any MAC address to be assigned to a VLAN, regardless of group association.

Partial configurations of the MAC to VLAN database can be downloaded to the switch using the timed download configuration feature. The MAC-to-VLAN database is stored in volatile memory only! On reboot the database will have to be loaded again. This can be automated by enabling timed download.

© 2001 Extreme Networks,Inc. All rights reserved

MAC-Based VLANs

- **Allow physical ports to be mapped to a VLAN based on the source MAC address learned in the FDB**
- **A port can only have a single endstation/host connected** (not good for Hub)
- **You may configure the source MAC address-to-VLAN mapping either offline, or dynamically on the switch**
- **Timed download configuration feature can be used to assist MAC to VLAN database configuration**
  * download MAC address from server

Notes:

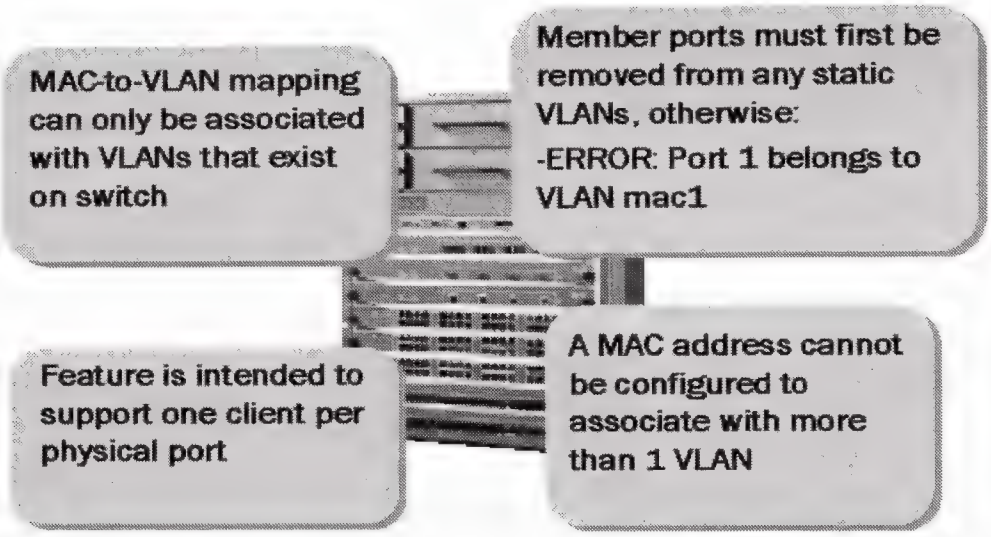
AC-Based VLAN Limitations

The following list details some of the limitations of MAC-based VLANs:

- Member ports must first be removed from any static VLANs
- The MAC-to-VLAN mapping can only be associated with VLANs that exist on the switch
- A MAC address cannot be configured to associate with more than 1 VLAN
- If this is attempted, the MAC address is associated with the most recent VLAN entry in the MAC-to-VLAN database
- Once a client MAC address has successfully registered, the VLAN association remains until the port connection is dropped or the FDB entry ages out
- A port can only have a single endstation/host connected

© 2001 Extreme Networks,Inc. All rights reserved

MAC-Based VLAN Limitations


MAC-to-VLAN mapping can only be associated with VLANs that exist on switch
Member ports must first be removed from any static VLANs, otherwise:
-ERROR: Port 1 belongs to VLAN mac1
Feature is intended to support one client per physical port
A MAC address cannot be configured to associate with more than 1 VLAN

Notes:

MAC-Based VLAN Configuration

Listed below are the steps that will enable you to configure MAC-based VLANs:

The first step is to create a MAC-based VLAN.

CLI Command – MAC-based port enabled
enable mac-vlan mac-group [any | <group_number>] ports <port number>
Enables a port to use the MAC-based VLAN algorithm. When a port is enabled to use the MAC-based VLAN algorithm, it will become a member of the MacVlanDiscover VLAN.

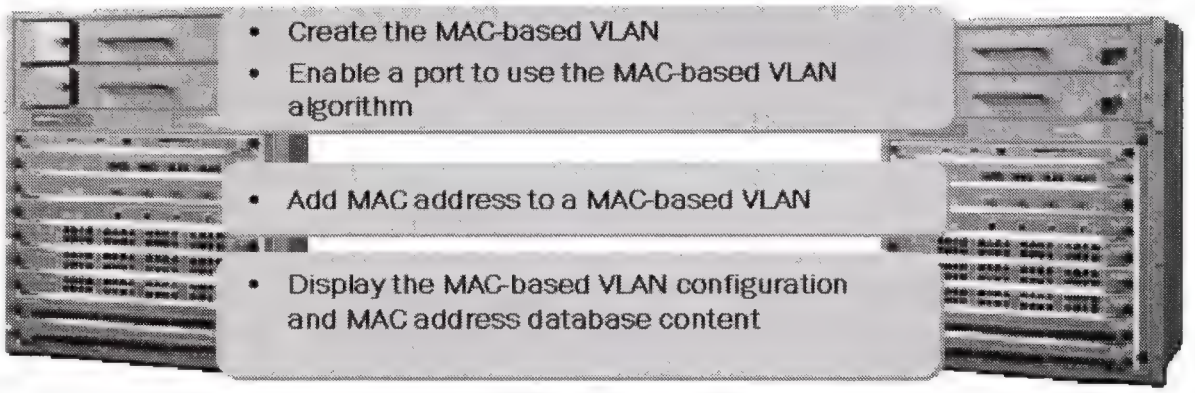
CLI Command – add MAC address
config mac-vlan add mac-address [any | <hex octet>] mac-group [any | <group_number>] vlan <vlan name>
Adds MAC address to a MAC-based VLAN.

Conference Rooms (a lot of ports)

CLI Command – show mac-vlan
show mac-vlan {configuration | database}
Displays the MAC-based VLAN configuration and MAC-based address database content.

© 2001 Extreme Networks,Inc. All rights reserved

MAC-Based VLAN Configuration


• Create the MAC-based VLAN
• Enable a port to use the MAC-based VLAN algorithm
• Add MAC address to a MAC-based VLAN
• Display the MAC-based VLAN configuration and MAC address database content

Notes:

MAC-Based VLAN Centralised Control

The Timed Configuration Download facility allows for centralised control of MAC-Based VLANs over multiple switches. It does this by controlling the downloads of incremental configuration files from a primary or secondary server at specified time intervals:

- If the switch is rebooted, the MAC-based VLAN configuration is automatically downloaded immediately after booting
- Timed downloads are configurable in 24 hour intervals

CLI Command – config download server
config download server [primary | secondary] <host_name/ip> <filename>
Configures the primary or secondary server and file name.

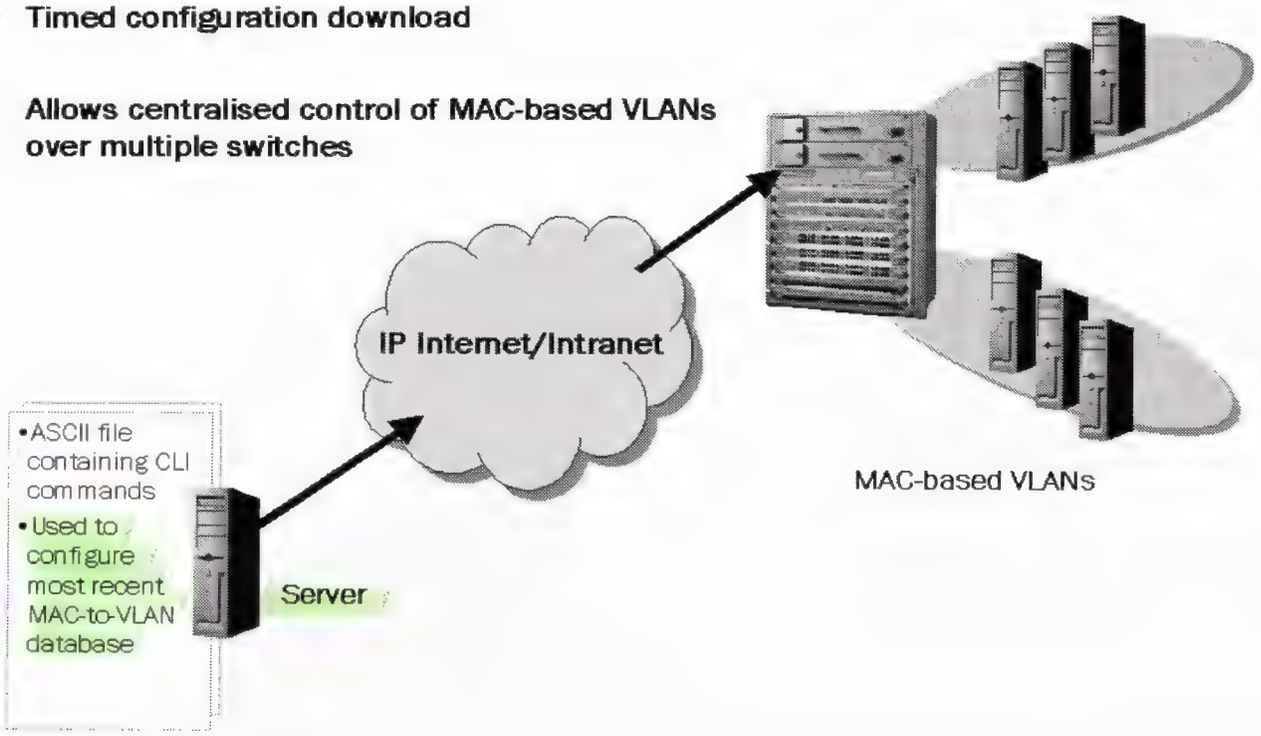
CLI Command – download configuration
download configuration every <hour (0-23)> <minute (0-59)>
Downloads timed interval configuration.

CLI Command – show download information
show switch
Displays timed download information.

© 2001 Extreme Networks,Inc. All rights reserved

MAC-Based VLAN Centralised Control

- **Timed configuration download**
- **Allows centralised control of MAC-based VLANs over multiple switches**



Notes:

Protocol-Based VLAN

When you configure this type of VLAN on the Extreme Networks switch, it enables filtering by protocol type in order to match a data stream to a particular VLAN.

Protocol-based VLANs enable the administrator to define a packet filter that the switch uses as the matching criteria to determine if a particular packet belongs to a particular VLAN.

Protocol-based VLANs are most often used when network segments contain hosts running multiple protocols, like the example shown in the diagram, where an ingress port is configured to receive traffic from three different protocol types (for example, IPX, IP and AppleTalk).

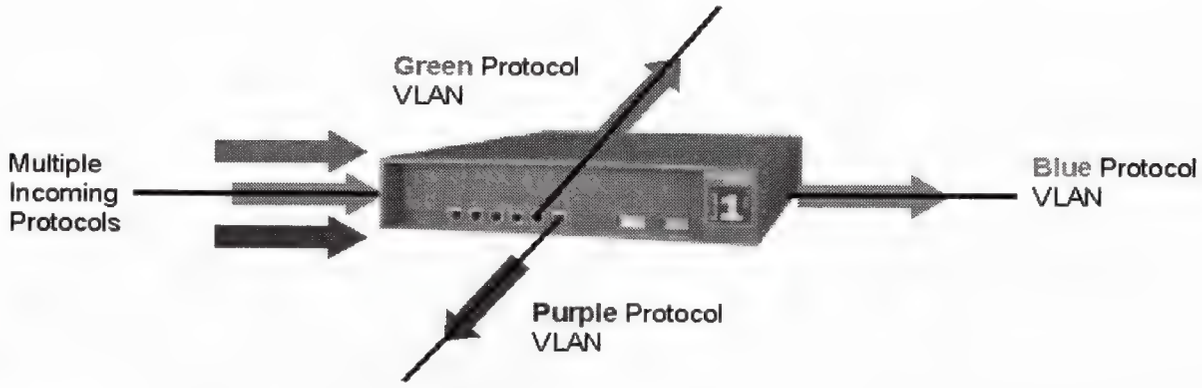
You can, of course, define packet filters that are customised to your exact requirements. However, the Extreme Networks switch family provides a range of pre-defined protocol filters for ease of implementation:

- IP
- IPX
- NetBIOS (Microsoft → NetBeui ← not routable)
- DECNet
- IPX_8022
- IPX_SNAP
- AppleTalk

© 2001 Extreme Networks,Inc. All rights reserved

Protocol-Based VLAN

- **It enables one to define a protocol filter to be used as the matching criteria to determine if a particular packet belongs to a particular VLAN.**



- **Or use the pre-defined protocol filters on the switch**

Notes:

Protocol-Based VLAN - Pre-defined Filters

If necessary, you can define a customised protocol filter based on the EtherType field, Logical Link Control (LLC), and/or Subnetwork Access Protocol (SNAP). Up to eighteen protocols may be part of a protocol filter.

The following procedures are used to define and configure a customised protocol filter:

CLI Command – create filter name
create protocol <protocol_name>
Creates a protocol filter, protocol names can have a maximum of 32 characters.

CLI Command – config filter
configure protocol <protocol_name> add [etype | llc | snap] <hex_value>
Configures the protocol filter. Supported protocol types include:

- etype - EtherType
- llc - LLC Service Advertising Protocol (SAP)
- snap - EtherType inside the IEEE SNAP packet encapsulation

CLI Command – delete filter
configure protocol <protocol_name> delete [etype | llc | snap] <hex_value>
Deletes a previously configured filter.

Note: The maximum number of simultaneously active protocol filters that can be active and configured for use as of EW 6.1.8 Release Notes are:

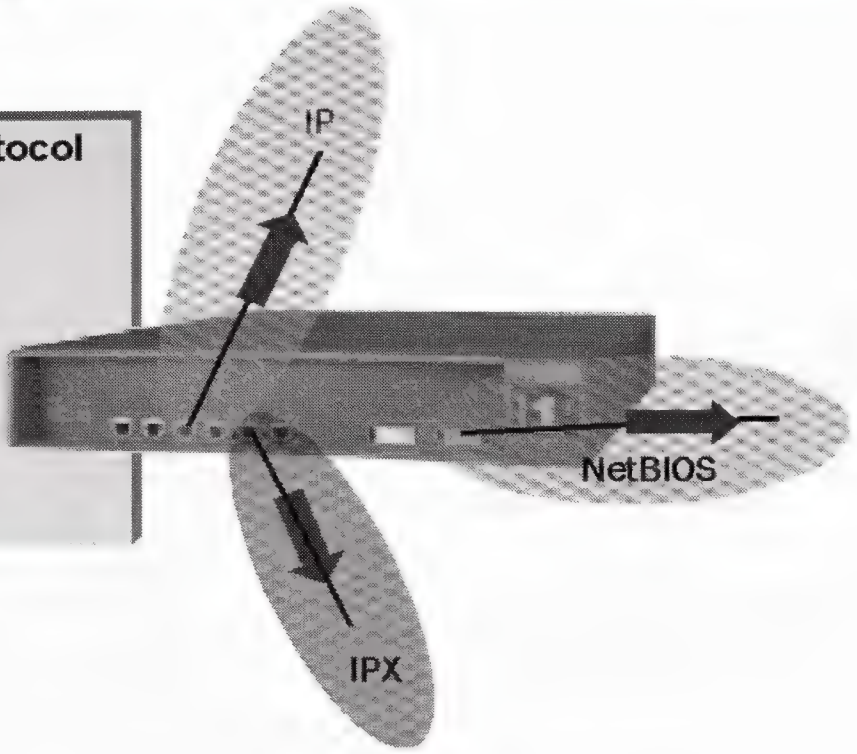
- *15 for i-based products*
- *7 for non-i based products*

© 2001 Extreme Networks,Inc. All rights reserved

Protocol-Based VLAN

Pre-defined Filters

- **Pre-defined Protocol Filters**
  - IP
  - IPX
  - NetBIOS
  - DECNet
  - IPX_8022
  - IPX_SNAP
  - AppleTalk



Notes:

Protocol-Based VLAN (L2) Example

The diagram shows protocol-based VLANs in use in a Layer 2 network environment.

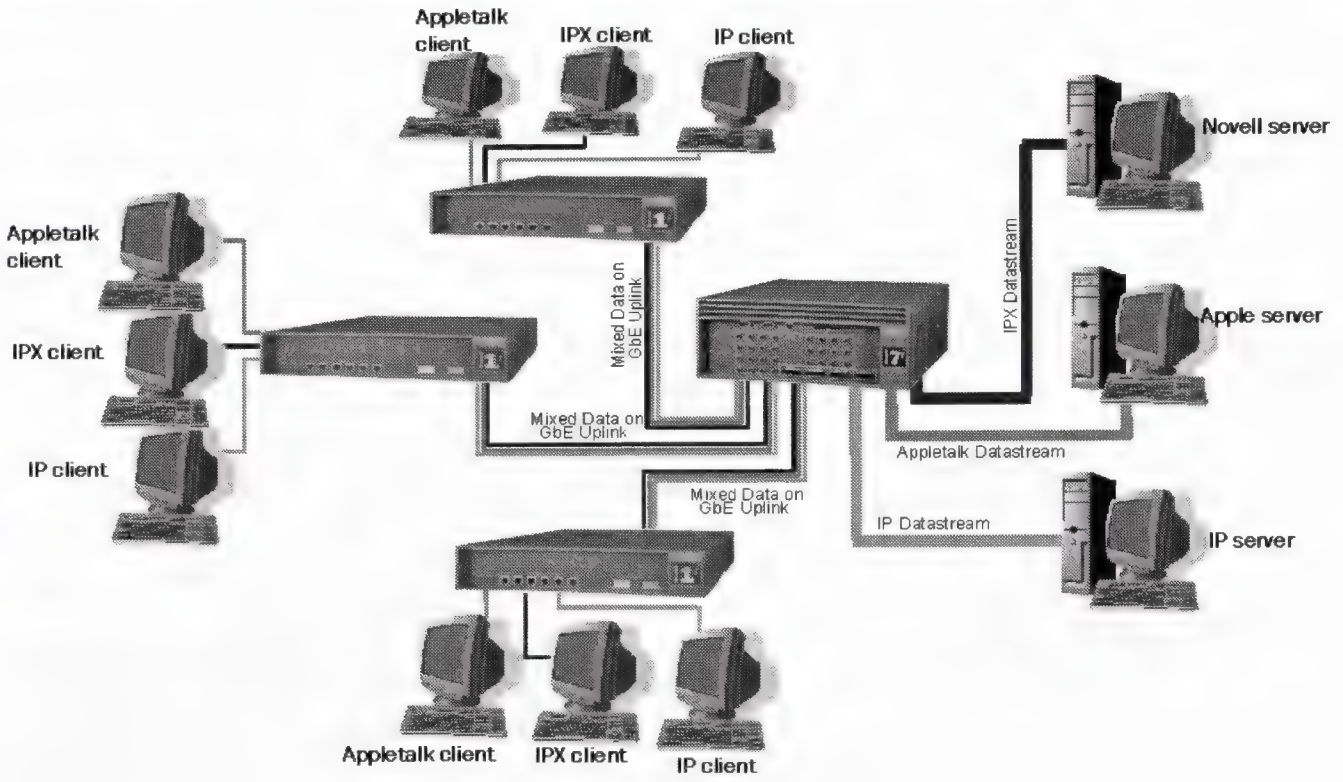
In this example we will protect the IP server in the orange VLAN from the traffic coming from the green and blue VLANs

The Extreme Networks Summit7i is the Core switch, and we will create three protocol-based VLANs as follows:

- VLAN Blue - IPX based VLAN
- VLAN Green – AppleTalk based VLAN
- VLAN Orange – IP based VLAN

© 2001 Extreme Networks,Inc. All rights reserved

Protocol-based VLAN (L2) Example



Notes:

VLAN (L2) Example Continued

Continuing with the example presented in the previous slide, we will now focus on the Summit7i at the Core and configure three Protocol-based VLANs, one for each protocol.

Each VLAN will consist of four ports; three of the ports will be connected to the Summit1i's and the remaining one is connected to the appropriate server.

Note that in this example, all three VLANs will have three ports in common - those serving the Summit S1i's at the perimeter. To accomplish this, three, protocol-sensitive VLANs will need to be created in the Summit7i's. The example commands are:

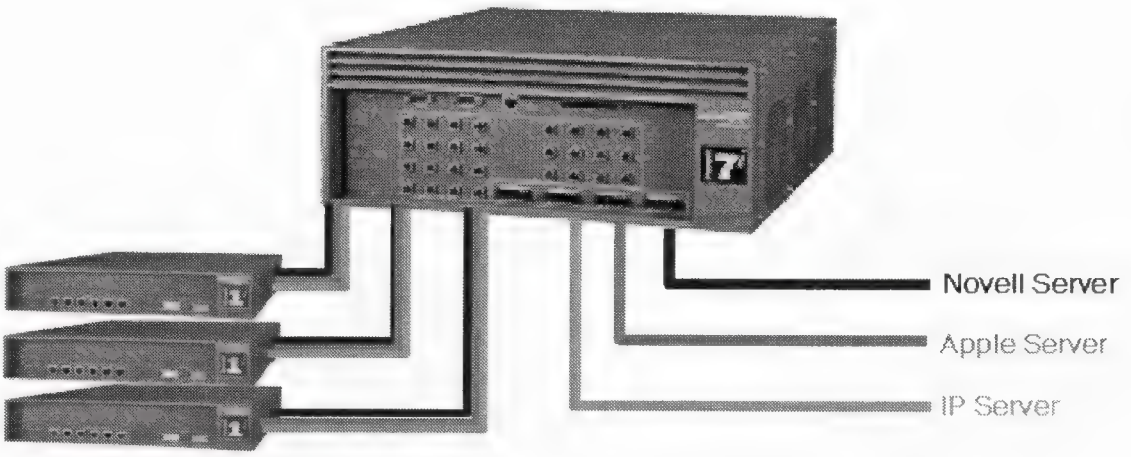
- create vlan IP_orange
- configure vlan IP_orange protocol ip
- configure vlan IP_orange add ports 17-20
- create vlan Atalk_green
- configure vlan Atalk_green protocol appletalk
- configure vlan Atalk_green add ports 17-19, 21
- create vlan IPX_blue
- configure vlan IPX_blue protocol ipx
- configure vlan IPX_blue add ports 17-19, 22

Remember, in this example, we are protecting the IP server in the orange VLAN from the traffic coming from the green and blue VLANs.

© 2001 Extreme Networks,Inc. All rights reserved

VLAN (L2) Example continued

- **Configure 3 Protocol-based VLANs, each with four ports**
  - All three VLANs will have three ports in common -- those serving the Summit S1i's at the perimeter



Notes:

Protocol-Based VLAN - Things to Remember

- Remember, you can only assign one protocol filter to a VLAN. The protocol filter is considered like a tag, i.e. one tag per VLAN
- When a protocol filter is deleted, the VLANs which had the protocol filter assigned are now assigned a protocol filter of none
- Precedence of Tagged Packets over Protocol Filters:
- If a VLAN is configured to accept tagged packets on a particular port, incoming packets that match the tag configuration take precedence over any protocol filters associated with the VLAN

  Example:

  When a packet is received on the port configured as VLAN purple with a Tag = 10 and VLAN green with an IPX protocol filter, which will the switch service first? The tag takes precedence when there is a match.

- When a new VLAN is created, it is assigned the "any" protocol by default. This means that the VLAN will forward traffic independent of the protocol type. If you want to remove the protocol filter from a VLAN, you should assign the "any" protocol to the VLAN

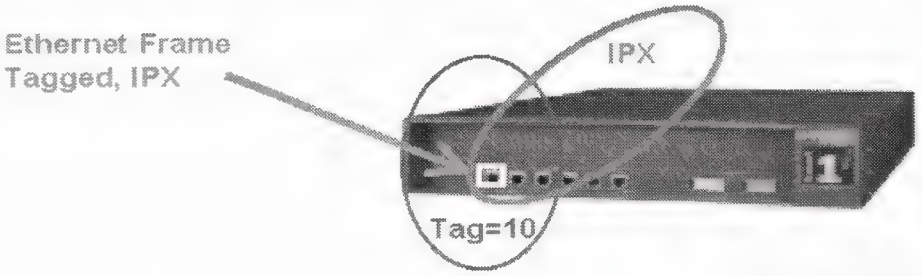
CLI Command – remove a protocol filter
config vlan <vlan_name> protocol any

protocol none (no traffic will got through)

© 2001 Extreme Networks,Inc. All rights reserved

Protocol-Based VLANs

Things to Remember



- **When a new VLAN is created, it is assigned the 'any' protocol by default**
- **When a protocol filter is deleted, the VLANs which had the protocol filters assigned are now assigned a protocol filter of none**
  - No traffic is forwarded until a protocol is assigned
- **Tagged packets take precedence over protocol filters associated with a VLAN**

Notes:

vMANs Explained - The Problem

What the customer wants:
Customers have a typical need to take the VLANs that are configured on local switches and replicate them on remote switches – using a Metropolitan Area Network (MAN) to interconnect them. In other words a transparent connection is required through the MAN, as if the customer had its own private cable.

What the MAN provider has:
The MAN service provider has a metropolitan network consisting of high performance core switches linked together with high-speed backbone circuits.

A vMAN is a feature that permits the tunnelling of any number of IEEE 802.1Q (and/or Cisco ISL) VLANs into a single VLAN. This traffic can then be switched through an Extreme Networks Ethernet infrastructure.

The vMAN feature is also useful in building transparent private networks that need point-to-point (or point-to-multipoint) connectivity across an Ethernet infrastructure.

On the Extreme Networks switch you create tunnels by creating VLANs and configuring member ports as:

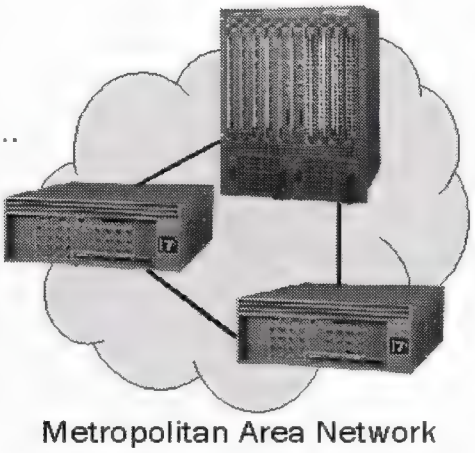
- Tagged on switch-to-switch ports
- Untagged on the tunnel's ingress/egress ports

© 2001 Extreme Networks,Inc. All rights reserved

vMANs Explained –The Problem

What the customer wants...

What the MAN provider has...



Metropolitan Area Network

Notes:

vMANs Explained - The Solution

The solution to this problem is to configure on the MAN switches, a VLAN (vMAN) so that the customer is provided with a transparent tunnel linking local and remote sites together.

This is achieved by changing the IEEE 802.1pQ Ethertype to hex 9100 (this configuration is performed only on the MAN switches). You must then enable jumbo frames on the MAN switches, because the Ethernet frame size is being extended past the accepted limit. The customer can then configure their switches as if they were directly connected.

Detailed below are the steps to configure a vMAN tunnel:

CLI Command – modify Ethertype
config dot1q ethertype <hex number>
Modifies the 802.1Q Ethertype used by switch to recognise tagged frames.

CLI Command – configure jumbo frames
config jumbo-frame size <framesize>
Configures the switch to accept jumbo frames.

CLI Command – enable switch for jumbo frames
enable jumbo-frame ports [all | <port number>]
Enables the switch to accept jumbo frames.

The slide shows an example configuration setup with vMANs. A tunnel has been created that have ingress/ egress ports on each Summit7i. For all the Extreme Networks Summit7i's that are shown, the configuration is:

default ethertype 81

- config dot1q ethertype 9100
- enable jumbo-frame ports <port numbers>
- config jumbo-frame size 1530
- create vlan Tunnel1
- config vlan Tunnel1 tag 40
- config vlan Tunnel1 add ports <port numbers> untag
- config vlan Tunnel1 add ports <port numbers> tagged

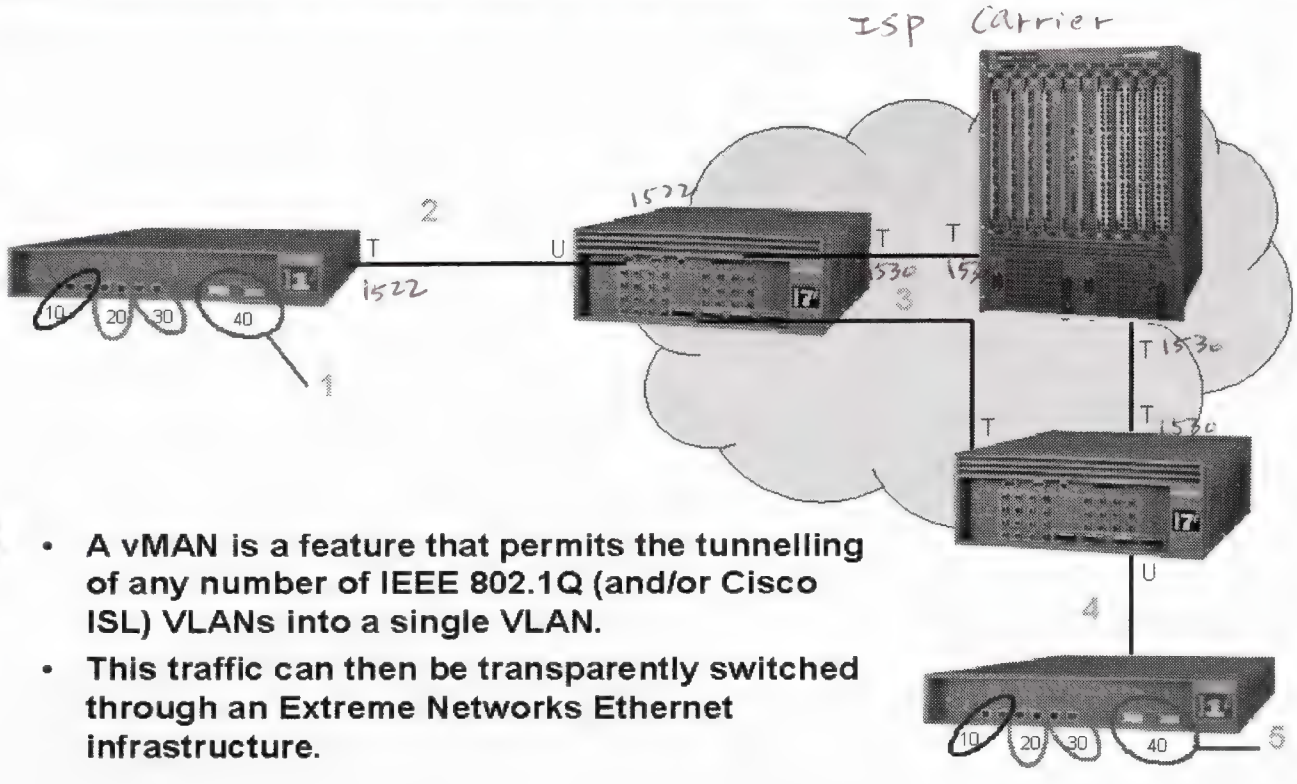
dot1p - dot1 priority
dot1q - dot1 tag

On the BlackDiamond:

- config dot1q ethertype 9100
- enable jumbo-frame ports all
- config jumbo-frame size 1530 create vlan tunnel1
- config vlan tunnel1 tag 40
- config vlan tunnel1 add ports <port numbers> tagged

© 2001 Extreme Networks,Inc. All rights reserved

vMANs Explained-The Solution



- A vMAN is a feature that permits the tunnelling of any number of IEEE 802.1Q (and/or Cisco ISL) VLANs into a single VLAN.
- This traffic can then be transparently switched through an Extreme Networks Ethernet infrastructure.

Notes:

vMANS Explained - The Result

1. A standard Ethernet frame comes in on an untagged port of an Ethernet switch. The incoming port is an untagged member of a VLAN with an 802.1Q ID of 40.

2. When the frame leaves the first switch via a tagged port, it will be tagged with a normal 802.1pQ tag, with a TPI of hex 8100 and a VLAN id of 40. When this frame reaches the vMAN switch, this switch does not recognize the frame as a tagged one, because the TPI is not equal to hex 9100. Therefore it treats the frame as an untagged frame. The incoming port is an untagged member of a VLAN with id 5. This VLAN is used as the vMAN for this customer.

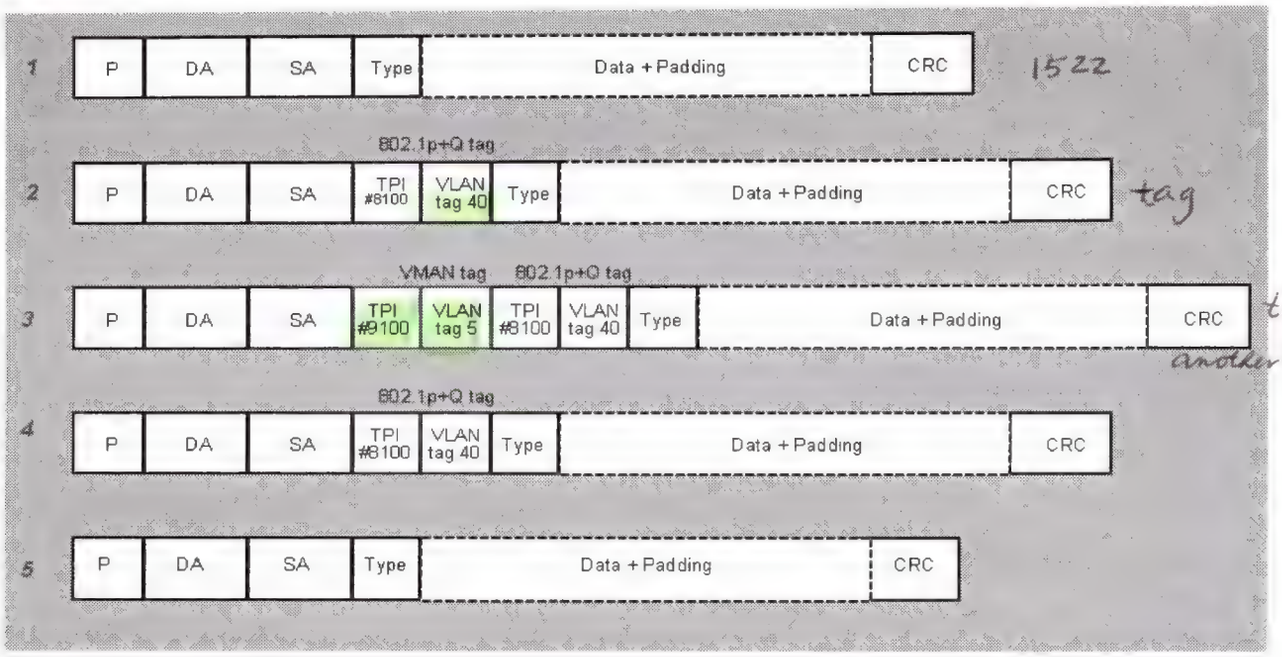
3. Traffic traversing the MAN via tagged ports carries a tag with a TPI of hex 9100. These frames are recognised by all vMAN switches as tagged frames. All traffic of the customer in this example is identified by tag value 5.

4. The frame leaves the MAN-edge switch. The tag (TPI 9100) is removed because the transmitting port is untagged. What is left is the standard 802.1pQ frame, which is recognized by the customer switch as a frame for VLAN id 40.

5. The customer switch treats the frame in a standard way, stripping of the 802.1pQ tag for an untagged port.

© 2001 Extreme Networks,Inc. All rights reserved

vMANs Explained – The Result



Notes:

Types of VLANs - A Review

VLANs can be created on the Extreme Networks switch according to the following criteria:

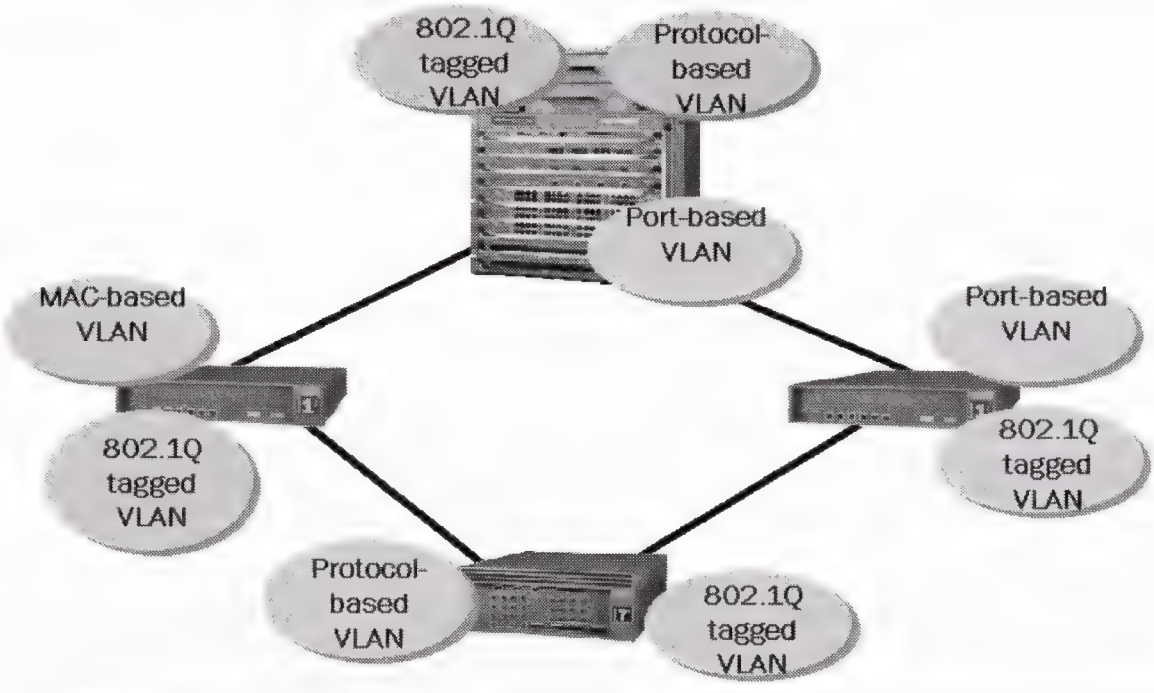
- Port-based (Untagged) VLAN
- 802.1Q Tagged VLAN
- Protocol-based VLAN
- Ethernet, LLC SAP, or LLC/SNAP Ethernet protocol type
- Treated like a Tagged VLAN
- MAC-based VLAN (MAC address)
- A combination of any of the above

In order for a port to participate in more than one VLAN, there must be a way for the switch to identify to which VLAN the traffic belongs. This can be achieved by using tagging or protocol filters

- Any number of VLANs can exist on a physical port (64 stated max), but only one may be port based (untagged)
- In other words, a port can simultaneously be a member of one port-based VLAN and multiple protocol or tag-based VLANs
- Traffic exiting the switch will follow the configured tag
- An error message will result if you attempt to add an untagged VLAN to a port with an existing untagged VLAN
- VLAN Default is the initial owner of all ports. To assign ports to a newly created VLAN, it is necessary to remove the ports from the default VLAN
- Use VLAN names consistently across the entire network
- Up to 3000 VLANs are supported

© 2001 Extreme Networks,Inc. All rights reserved

Types of VLANs – A Review



- **Additionally: VMANs allow 'tunnelling' of 802.1Q and/or Cisco ISL VLANS into a single core**

Notes:

Summary

Chapter six has examined the different types of VLANs that may be configured on the Extreme Networks switch product family. You should now be able to:

- Define VLANs in an overview
- Describe VLANs in Extreme Networks Switches
- Distinguish between VLAN types - port-based, tagged, MAC-based, protocol-based, and vMANs
- Configure:
- Port-based VLAN
- VLAN tagging on an Extreme Networks Switch
- MAC-based VLAN
- Define Protocol-based VLANs
- Explain vMAN and Jumbo Frames
- Successfully complete the lab exercises

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Summary

You should now be able to:

- **Define VLANs in an overview**
- **Describe VLANs in Extreme Switches**
- **Distinguish between VLAN types: port-based, tagged,MAC-based,protocol-based, and vMANs**
- **Configure**
  - Port-based VLAN
  - VLAN tagging on an Extreme Switch
  - MAC-based VLAN
- **Define Protocol-based VLANs**
- **Explain vMAN and Jumbo Frames**
- **Successfully complete the lab exercises**

Notes:

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 7

Spanning Tree Configuration

Chapter Objectives

Chapter seven explains what the Spanning Tree Protocol (STP) is used for and how it works. The chapter determines the exact building blocks of the spanning tree protocol and how spanning tree is configured on the Extreme Networks switch products.

Upon completion of this chapter you will be able to:

- Define spanning tree protocol in an overview
- Explain how spanning tree works
- Determine the building blocks of STP
- Describe ports, VLANs, STPD relationship
- Configure STP on an Extreme Networks switch

Successfully complete the lab exercises on STP configuration

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

Upon completion of this chapter, you will be able to:

- **Define Spanning Tree Protocol in an overview**
- **Explain how Spanning Tree works**
- **Determine the building blocks of STP**
- **Describe Ports, VLANs, STPD relationship**
- **Configure STP on an Extreme Networks Switch**
- **Successfully complete the lab exercises on STP configuration**

Notes:

Spanning Tree

What is the Spanning Tree Protocol?
The spanning tree protocol is a network management protocol that is used to prevent loops in a redundant network topology. Spanning tree uses the Spanning Tree Algorithm (STA) to calculate the best switch path through the network. The spanning tree protocol shares this information with other switches on the network using frames called Bridge Protocol Data Units (BPDUs). These management control frames are used to exchange STA calculations between the switches. Using the information provided by the BPDUs, the spanning tree protocol can then "prune" any redundant paths.

The spanning tree protocol, originally developed by the Digital Equipment Corporation (DEC) is described in the original documents as a bridge-based mechanism for providing fault tolerance on networks. Spanning tree allows you to implement parallel paths for network traffic, and ensure that:

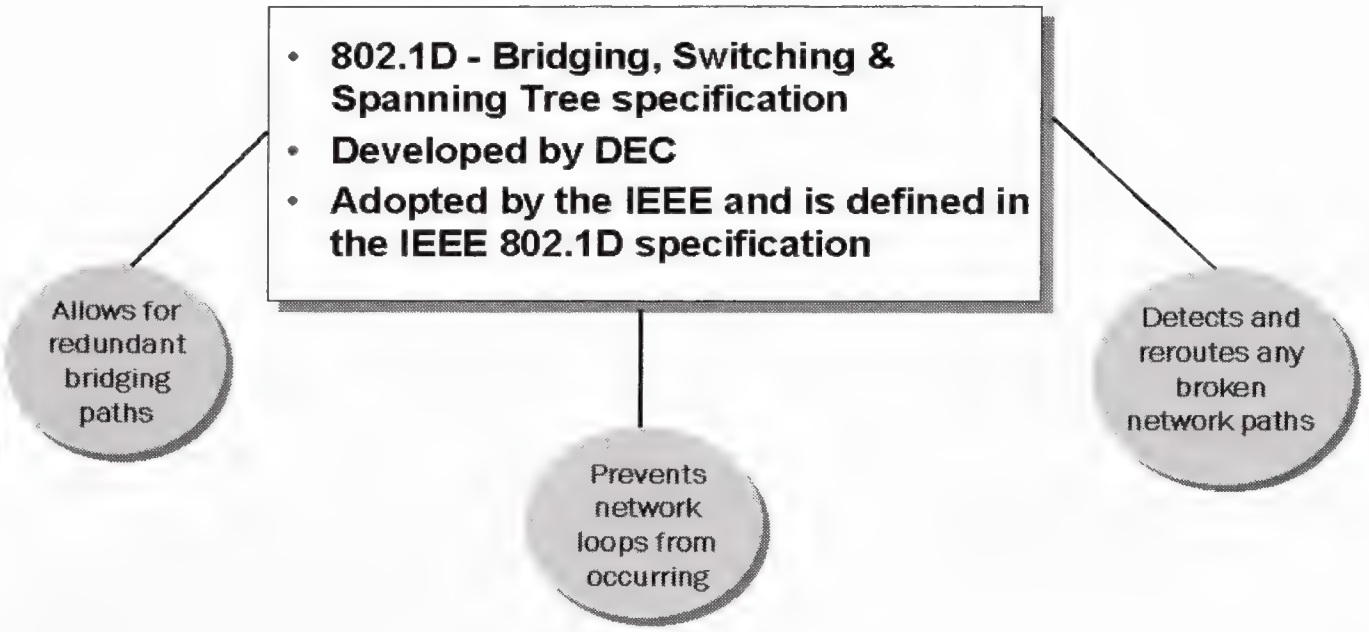
- Redundant paths are disabled when the main paths are operational
- Redundant paths are enabled if the main path fails
- Spanning tree has been adopted by the IEEE committees to run on any LAN topology

Spanning tree is a protocol that performs the task of, amongst other things, providing fault tolerance on networks, and should not be confused with the functions of a transparent bridge. Most transparent bridges support and also run the spanning tree protocol and this is sometimes where the confusion arises.

NOTE: STP is a part of the 802.1D bridge specification defined by the IEEE. To explain STP in terms used by the 802.1 specification, the Extreme Networks Summit and BlackDiamond Switches will be referred to as bridges.

© 2001 Extreme Networks,Inc. All rights reserved

Spanning Tree


802.1D - Bridging, Switching & Spanning Tree specification
Developed by DEC
Adopted by the IEEE and is defined in the IEEE 802.1D specification
Allows for redundant bridging paths
Prevents network loops from occurring
Detects and reroutes any broken network paths

Notes:

Spanning Tree Algorithm

Physical loops are created in a switched network when two network segments are connected by two, or more, Layer 2 switches form a circular path.

Bridges and switches are designed to "flood" Ethernet broadcasts and unknown traffic (where the destination is unknown and so must be sent out on each port). This causes the potential for traffic to loop around the network.

When a broadcast frame is received on a switch port, the frame is re-transmitted out of every switch port (unless the switch ports are assigned to different VLANs). If the LAN network contains multiple paths, it can result in the broadcast frame being sent back and forth between the switches. This is often referred to as a broadcast storm, and broadcast storms grow exponentially and can bring a network down.

To prevent broadcast storms, the Spanning Tree Protocol (STP) eliminates redundant paths by placing only one switch port in forwarding mode and placing all other ports connected to the same segment in blocking mode.

Thus, the rules for spanning tree are based on the following:

- Bridged networks must allow for redundancy
- Only one path should be enabled to any destination on the network

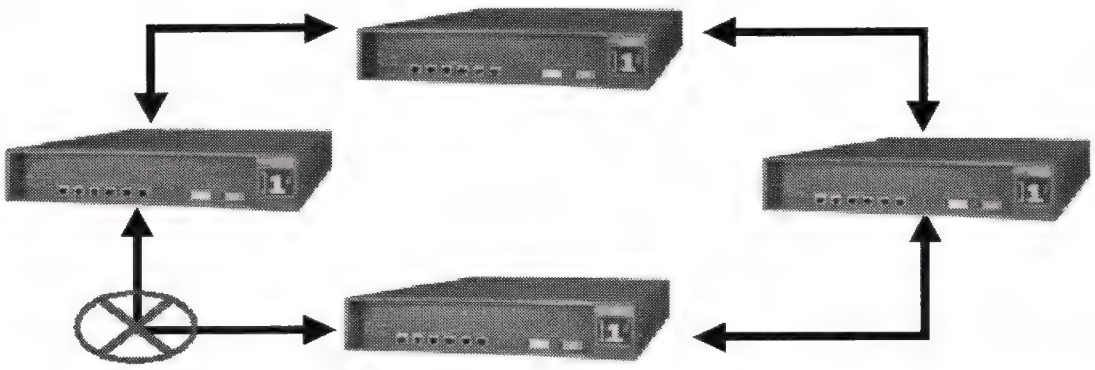
The spanning tree algorithm dynamically configures a loop-free active topology from the connected components of a bridged LAN.

Some of the ports on the bridges in the network will forward frames, whilst other ports will be instructed not to forward frames. Ports that are allowed to forward frames are put into what is called the "forwarding" state. Whilst ports that are instructed not to forward frames are put into what is called the "blocking" state (however, these ports will still participate in the Spanning tree protocol)

Prior to spanning tree being adopted, the network had either to be carefully designed to ensure that no loops were present in the network configuration, or, use a proprietary algorithm provided by the bridge vendor.

© 2001 Extreme Networks,Inc. All rights reserved

Spanning Tree Algorithm



- **Bridged networks must allow for redundancy**
- **Only one path should be enabled to any destination on the network**
- **Certain ports are allowed to forward packets**
  - Other ports will participate in spanning tree but do not forward packets

Notes:

Reconfiguration in Spanning Tree

Spanning tree maintains an active topology, which will re-configure the network automatically if there is a topology change caused by, for example, a link up or link down situation.

What happens when a link fails?
One of the most important features of any critical network is redundancy. If the job of the spanning tree is to prune all of the redundant links, what happens if the active link fails?

Spanning tree sends out BPDUs at regular intervals. If there is a change in the status of a link, the BPDUs will report this change, and the spanning tree will then recalculate the best path through the network. The process of placing one active port in forwarding mode and blocking all other ports is then repeated until a stable, active topology is achieved.

Reconfiguration of the active topology will also be necessary as a result of the following:

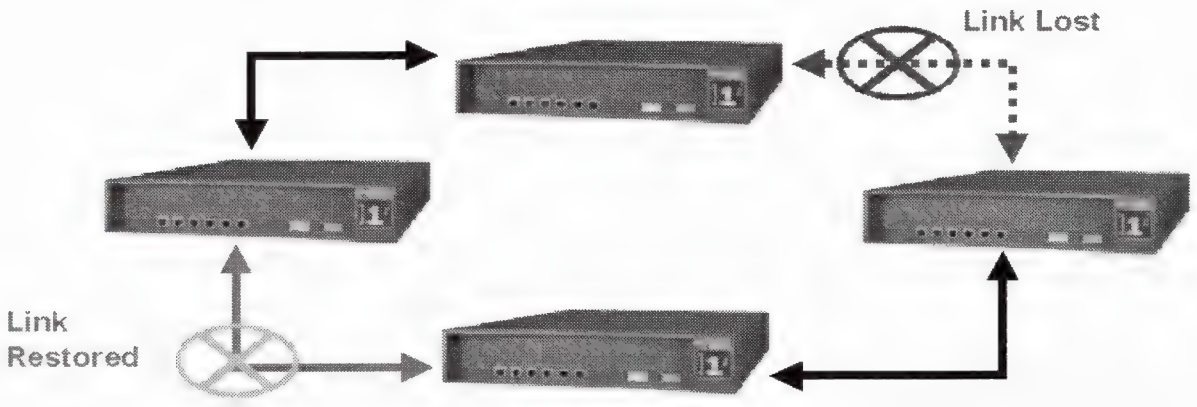
- Network components being removed
- An active bridge failing to forward packets
- Management changes being made to the active topology.

In the example shown, if one of the other links is lost, the link that was put into blocking mode by spanning tree, will now be put into forwarding mode to restore connectivity.

The following slides examines in more detail what happens when a reconfiguration occurs.

© 2001 Extreme Networks,Inc. All rights reserved

Reconfiguration In Spanning Tree



- **Occurs when there is a change in the active topology**

Notes:

How Spanning Tree Works - Root Bridge

To understand how the Spanning Tree works, it is important to understand the following terminology:

- Bridge ID, Root Bridge, and Root Port
- Designated Bridge and Designated Port
- Maintaining an Active Topology
- BPDU – Bridge Protocol Data Unit

As we proceed through chapter seven each one of these terms will be explained.

Each Spanning Tree Protocol Domain (STPD) (discussed later in detail) will have one Root Bridge, which will be the controlling source of all spanning tree communications. The root bridge is at the top level of the hierarchy (i.e. the root of the spanning tree) and will become the designated bridge for it's attached segments.

Determining the Root Bridge

The selection of the root bridge is based on the determination among connected bridges, using the Bridge ID. Basically, this means that if there are no configuration changes made to affect bridge selection, the bridge with the lowest MAC address will become the root bridge. The Bridge ID is an 8-octet number, consisting of the MAC address and a configurable bridge priority. The bridge priority field consists of 2-octets and are the most significant bits of the Bridge ID, these will be determinant when the bridges are configured differently. When bridge priorities are configured equal (as is often the case when bridges are left at their default values), the least significant part of the ID (MAC address) will be the tie-breaker.

When a spanning tree network is configured, the topology becomes active by each bridge initially transmitting Configuration Bridge Protocol data Units (CBPDU's) indicating that it is the root bridge. All bridges will receive this information and each will save the "best" information. The "best" information is based on three items in the CBPDU:

- The Root ID field,
- The Transmitting bridge ID, and
- The cost field

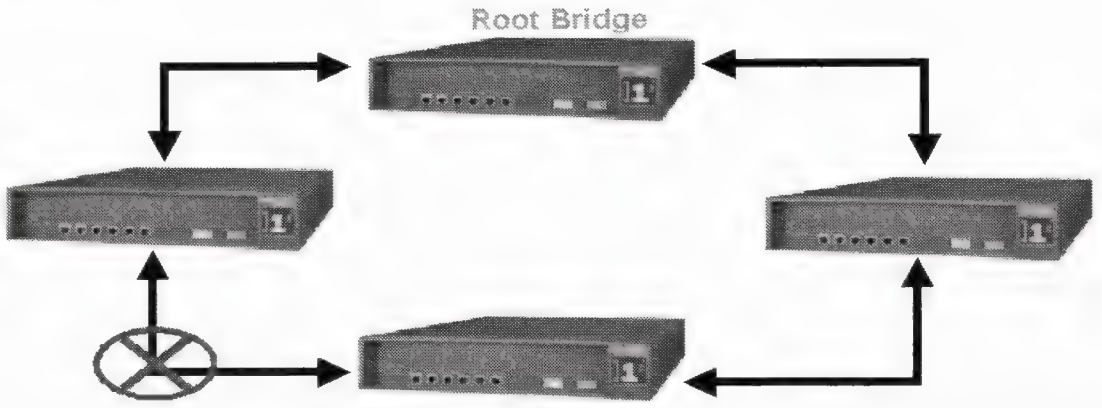
Example - A bridge that receives a topology message from another bridge will perform the following tests:

- If the root ID of the received CBPDU is of a better priority than the previously saved message (including its own), it will discard the previously saved CBPDU and keep the new one.
- If the root ID's are equal, check the cost. If the cost is lower, the previously saved message will be discarded and the new one kept.
- If the root ID's and costs are equal, compare the transmitter ID. If the new transmitter ID is lower, the previously saved message will be discarded and the new one kept.

© 2001 Extreme Networks,Inc. All rights reserved

How Spanning Tree Works

Root Bridge



- One bridge- the one with the highest priority (lowest bridge ID) will become the root bridge
- All ports on the root bridge are placed in the forwarding state
- This bridge is the root (source) of spanning tree

Notes:

How Spanning Tree Works - Root Port

Every bridge in the bridged LAN, with the exception of the root bridge, has a root port. The root port has the lowest cumulative cost to reach the root bridge.

In the active topology, other bridges that are not the root bridge will select a port with lowest path cost toward the root bridge. The definition of the root port is the port on a designated bridge that transmits to the root bridge.

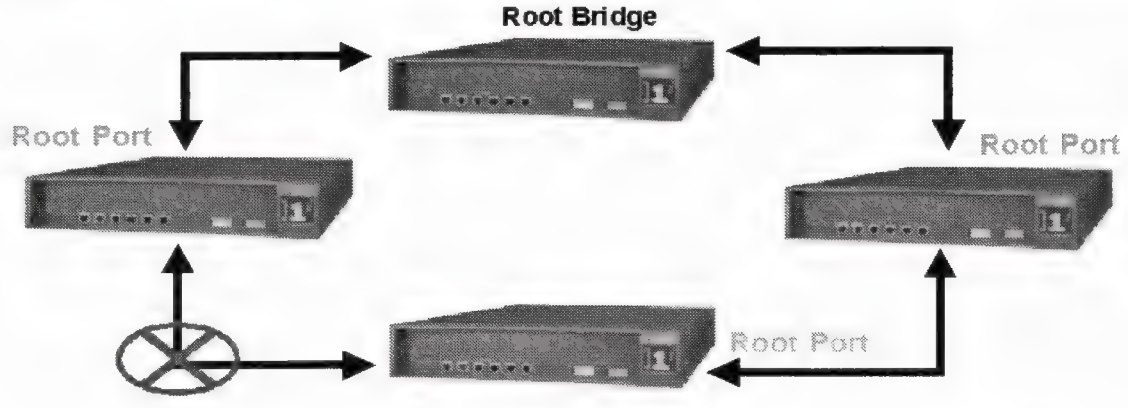
If a root port fails to receive timely CBPDU updates on it's root port, the spanning tree will reconfigure because either the root bridge has failed, or because an intervening bridge or link has gone down.

The root port is placed in the forwarding state, and there is only one root port per spanning tree per bridge, regardless of the number of ports in that tree. (ExtremeWare is no exception to this rule even though it allows for multiple trees per device).

© 2001 Extreme Networks,Inc. All rights reserved

How Spanning Tree Works

Root Port



- **Other bridges select a port with the lowest path cost to the root bridge**
  - This port becomes the root port and is placed in the forwarding state
  - There is only one root port per spanning tree per bridge, regardless of the number of ports in that tree.
  - EXCEPTION:
    - *ExtremeWare allows for multiple trees per device*

Notes:

How Spanning Tree Works - Designated Bridge

A designated bridge is the bridge attached on each LAN segment that has the lowest cumulative path cost to the root bridge. If more than one bridge on the segment has the same root path cost, the bridge with the lowest bridge ID becomes the designated bridge for the LAN.

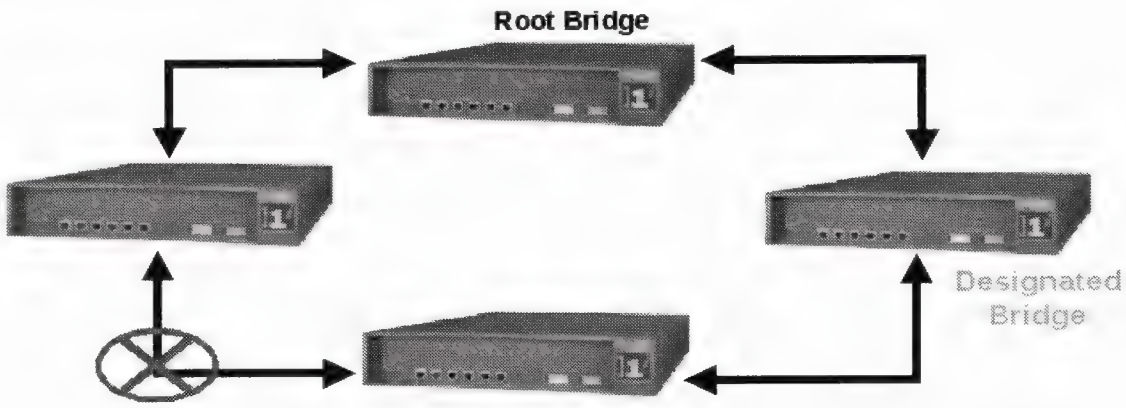
Each LAN segment will have it's own designated bridge offering the lowest path cost to the root bridge from that individual collision domain.

The port on the designated bridge that provides the best path to the root bridge for the LAN segment is the designated port.

© 2001 Extreme Networks,Inc. All rights reserved

How Spanning Tree Works

Designated Bridge



- **Selected as the bridge that provides a LAN segment with the lowest path cost to the root for that individual cable segment.**

Notes:

How Spanning Tree Works - Designated Ports

Designated Ports

The definition of designated ports, are the ports on a designated bridge that attach to the segments for which that bridge is the designated bridge.

Certain ports are identified as designated ports:

- These ports are placed in the forwarding state
- They are the designated best path to the root bridge

Blocking Ports

Other bridges or ports not selected have their ports placed in the "blocking" state:

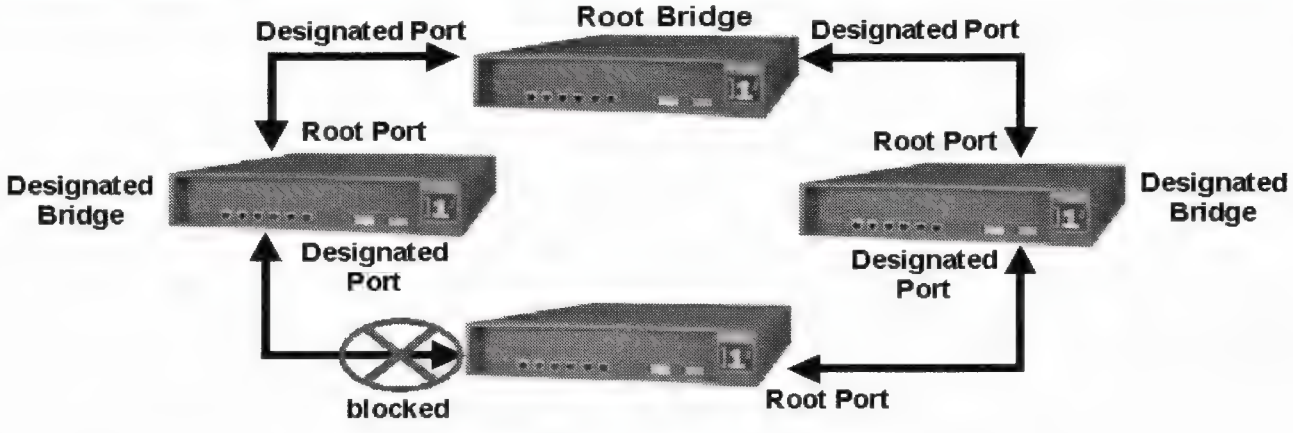
- The blocking state prevents data packets from being forwarded on that port
- These ports still participate in the spanning tree for future updates

If the path cost to the root bridge is the same for the two ports of the bottom bridge in the example, the port with the highest port ID (highest port number) will be blocked.

© 2001 Extreme Networks,Inc. All rights reserved

How Spanning Tree Works

Designated Ports



- Designated ports are placed in the forwarding state
  - They are the designated best path to the root bridge
- Those ports that are not selected, are placed in the blocking state
- The blocking state prevents data packets from being forwarded on that port – they still participate in spanning tree updates

Notes:

How Spanning Tree Works - BPDUs

A stable active topology is maintained by the root bridge - by transmitting configuration messages out on all of its active ports. The designated bridges should receive these PDU's on their root ports, and the designated bridges should then propagate the information out on all of its active ports.

BPDU (Bridge Protocol Data Unit)

This is a special protocol to maintain the overall spanning tree topology. Bridges will constantly communicate with each other about their status and any required configuration of the network. BPDU's are sent to the bridge group address (01:80:C2:00:00:00). The two types of BPDU's are:

- Configuration BPDU's
- Topology change BPDU's

Configuration BPDU

This is sent to all bridges from the root bridge. It is used to determine least cost path information and determine which bridge is the root bridge. The time out information is transmitted in the configuration messages to all bridges. The timeout value accounts for propagation delay through the bridges in the spanning tree.

Topology Change BPDU

Whenever a designated bridge detects a topology change, such as bridges being added or removed, the root bridge failing, or, manual configuration change of bridge parameters, it sends out a topology change BPDU through it's root port.

This information is eventually relayed to the root bridge. The root bridge then sets the topology change flag in it's CBPDU so that the information is sent to all bridges. It transmits this CBPDU for a fixed amount of time to ensure that all bridges are informed of the topology change.

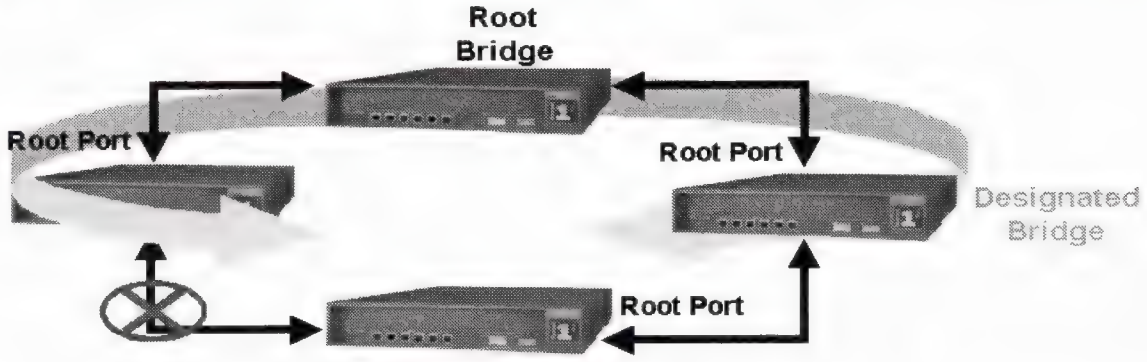
As a result the spanning tree is re-calculated. All bridges flush their forwarding database to ensure that each active port still forwards frames to the right network after a topology change.

© 2001 Extreme Networks,Inc. All rights reserved

How Spanning Tree Works

BPDUs

Layer 2 broadcast



- **A stable active topology is maintained by the root bridge**
- **The root bridge transmits configuration messages out of all of its active ports**
- **Spanning Tree Bridges communicate using:**
  - BPDU – Bridge Protocol Data Unit
  - Configuration BPDU
  - Topology change BPDU

Notes:

Building the Spanning Tree Domain

Calculation of the Root Bridge given RootID, Cost, Trasmitter ID

Four Ethernet segments and five bridges are to configure a loop free topology. The first rule in the spanning tree algorithm is that one bridge must become the root bridge.

Upon initialisation, each bridge will transmit a topology message indicating that it is the root bridge:

- The numbers on each bridge port show the root topology message that the bridge sends out when determining the root bridge.

Bridge 1 will win the right to become the root bridge, because the bridge ID of bridge 1 is 1 and it is the lowest of all the bridges. Bridge 1 will then transmit its topology message.

- All bridges receive bridge 1's topology message, save it, and propagate it to all other bridges.
- Eventually all bridges will keep this message which identifies bridge 1 as the root.

Calculation of the Participating Ports

Since the root bridge is now selected, each bridge must determine if it will become the designated bridge for any of the cable segments to which it is connected.

- The root bridge places its ports in the forwarding state.
- The root bridge is the designated bridge for cable segments 3 and 4.

Bridge 3 places one of its ports in the blocking state, because it is on the same cable segments as the root bridge. Remember, only one of its ports will be placed in the blocking state, and the decision criteria is the port ID.
Bridge 4 becomes the designated bridge for cable segment 2.

- It selects its root port and its designated port.

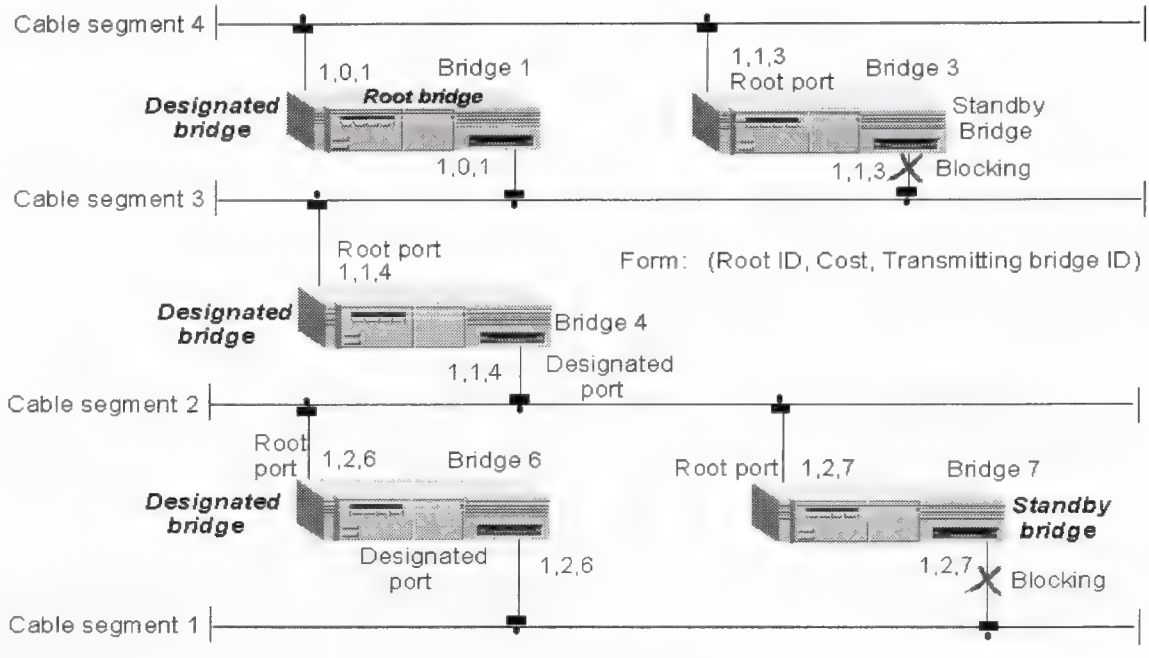
Bridge 6, and 7 have equal costs to the root bridge, and in this case the tie-breaker is based on the transmitting bridge ID:

- Transmitting bridge ID 6 is lower than 7, so bridge 6 becomes the designated bridge for cable segment 1, and selects a root port
- Bridge 7 places one of its ports in blocking mode, the decision being based on the port ID.

With a bridge that has more than two ports, it is possible for a single bridge to become designated on some cable segments to which it is connected and to place some of its other ports into blocking mode.

© 2001 Extreme Networks,Inc. All rights reserved

Building the Spanning Tree Domain



Notes:

Root Bridge Failure

The diagram shows an example of how the spanning tree domain re-configures itself after a change in the active topology – in this case the failure of the root bridge. Other component failures such as, port failure, link failure, and designated bridge failure will cause similar re-configuration changes to occur.

The spanning tree topology is kept active through the transmission of BPDU's, and every two seconds the root bridge will transmit a root bridge topology message (CBPDU) on all its active ports.

The "max age" timer specifies the maximum time in which a bridge should receive a BPDU:

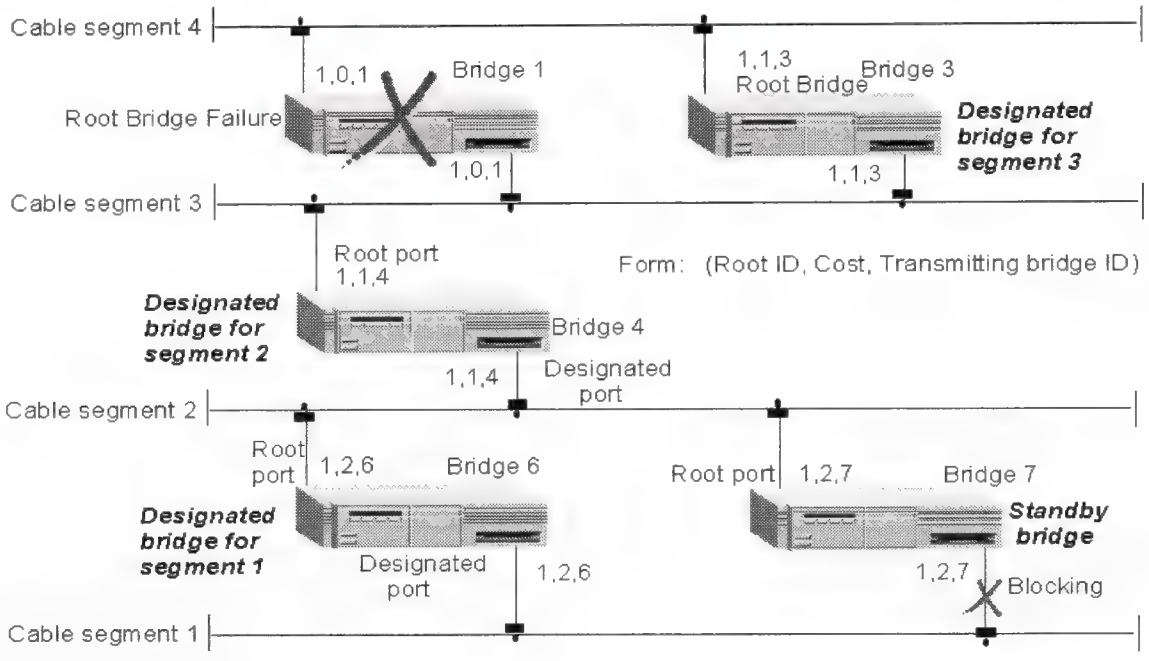
- The default of this timer of 20 seconds
- Whenever a bridge receives a BPDU, it resets the max age timer

If 20 seconds expire, then the bridge assumes spanning tree has failed and the bridge will go into convergence state. When this situation occurs, the same process that initially selected the original root bridge is used again to determine which bridge should now become the new root bridge.

- As bridge 3 has the lowest bridge ID, it becomes the root bridge for the domain

© 2001 Extreme Networks,Inc. All rights reserved

Root Bridge Failure



Notes:

Extreme Networks Switches and Spanning Tree

We have reviewed bridging concepts and the spanning tree algorithm and how it provides fault tolerance for our network implementation at layer 2.

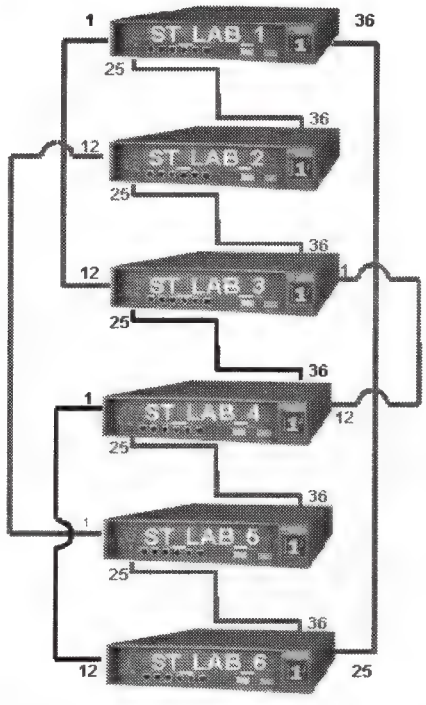
The remaining pages in this chapter discuss the Extreme Networks bridging and spanning tree implementation across the range of switches.

The diagram illustrates a physical network topology that will benefit if Spanning Tree is configured to prevent broadcast storms. If you examine the diagram closely, there are physical loops that exist.

© 2001 Extreme Networks,Inc. All rights reserved

Extreme Networks Switches and Spanning Tree

- **Multiple Domains**
- **STPD**
  - Spanning Tree Protocol Domain
  - S0 - default STPD
- **VLANs**
- **Things to remember**



Notes:

Multiple Domains and Spanning Tree

The Extreme Networks switches can be partitioned into multiple virtual bridges (Layer 2 interfaces represented by VLANs).

For example, continuing on with the diagram from the previous slide, what is shown here is a logical diagram of its equivalent.

Each spanning tree instance in the switch is called an STPD (Spanning Tree Protocol Domain or just Spanning Tree Domain) and as shown, we can configure the VLAN Redish and the VLAN Blue to each belong to a separate STPD, namely S1 and S0 respectively:

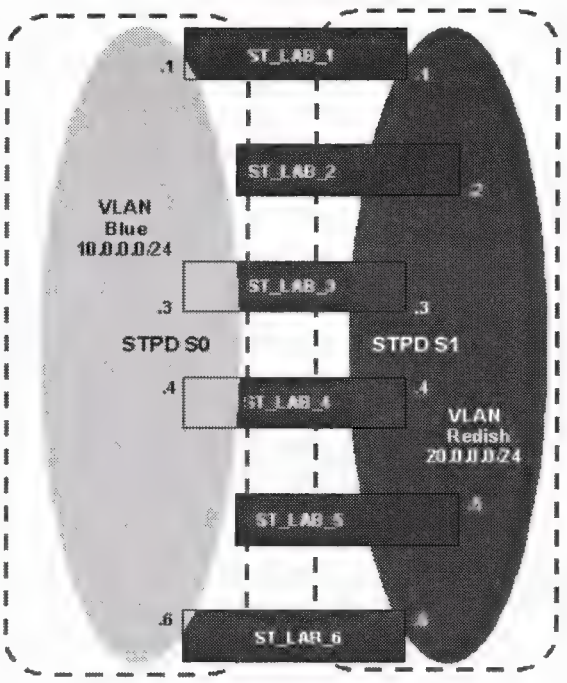
- Each STPD has its own Root Bridge and active path
- VLAN Blue on S0 will have a root bridge and so will VLAN Redish.

An Extreme Networks switch can have have up to 64 STPD's per switch.

© 2001 Extreme Networks,Inc. All rights reserved

Multiple Domains and Spanning Tree

- **The switch can be partitioned into multiple virtual bridges**
- **Each spanning tree instance in the switch is called an STPD**
  - STPD - Spanning Tree Protocol Domain or just Spanning Tree Domain
  - Extreme Networks supports 64 STPDs per switch
- **Each STPD has its own Root Bridge and active path**



Notes:

STPD "s0"

When a switch is shipped, it has one default STP called "s0", and by default the spanning tree is disabled on s0.

Spanning Trees have VLANs as members, meaning that VLANs are assigned to STPD's.

- All VLANs are automatically made members of "s0"

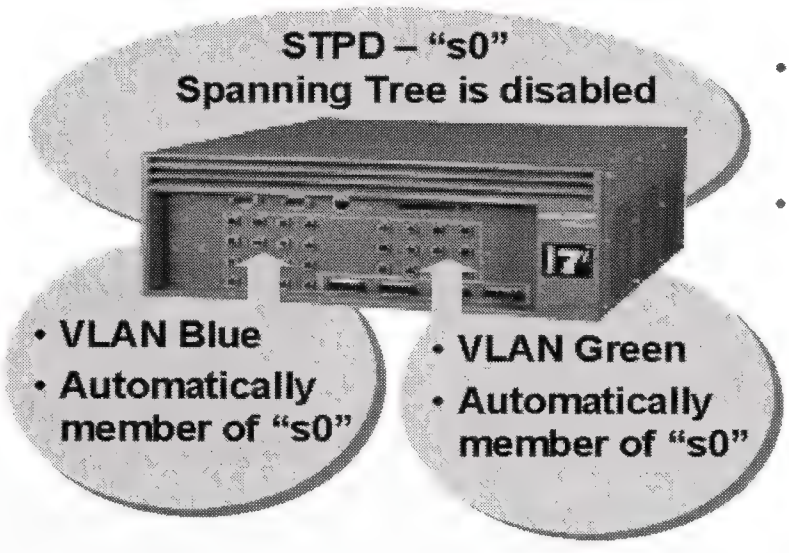
CLI Command – create STPD
create stpd <stpd_name>
Creates a new spanning tree protocol domain on the switch.

CLI Command – add vlan to STPD
config stpd <stpd_name> add vlan <vlan_name>
Assigns one or more VLANs to STPD (once STPD has been created).

NOTE: You cannot delete a VLAN from "s0", but you can add it to another STPD. You do this by moving the VLAN from s0 to the new STPD.

© 2001 Extreme Networks,Inc. All rights reserved

STPD "s0"



- Default switch configuration contains one STPD called "s0" and STP is disabled
- All VLANs are automatically made members of "s0"
- Spanning Trees have VLANs as members

Notes:

Ports, VLANS and STPD

A VLAN and port can belong to only one STPD. If a port is a member of multiple VLANs then all those VLANs must belong to the same STPD.

NOTE: Care must be taken to ensure that multiple STPD instances within a single switch do not see each other in the same broadcast domain. For example, this could happen if another external bridge is used to connect VLANs belonging to separate STPD's.

Example:

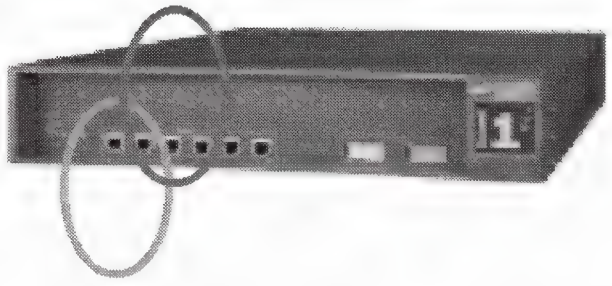
VLAN orange has ports 1 & 2 as member ports, and belongs to STPD S1

VLAN blue has ports 2-4 as members and is a tagged VLAN. Blue should also belong to S1 because port 2 is a member of S1 via Orange.

NOTE: When you try to add VLAN blue to a different STPD, you get the following error:ERROR: Cannot assign bridge to stpd!

© 2001 Extreme Networks,Inc. All rights reserved

Ports, VLANs, and STPD



- **A VLAN can only be a member of one STPD**
- **A physical port can belong to only one STPD**
- ***If a port is a member of multiple VLANs, then those VLANs must belong to the same STPD***

Notes:

Spanning Tree Configuration

"If a port is a member of multiple VLANs, then those VLANs must belong to the same STPD"

Though simple in approach, this can lead to several configuration "gotchas" and hence it is recommended to:

- Draw the physical network; if there is a loop anywhere, some link will get blocked
- Remove all VLANs associated with the STP before deleting the STPD
- If you delete an STPD, it will delete its' member VLANs!
- Spanning Tree is designed for Layer 2 environment where you can have redundant paths but only having one active path at a time to eliminate loops which eventually cause broadcast storms.
- STP and load-sharing do work together
- STP and the redundant physical port/link will work well together.

© 2001 Extreme Networks,Inc. All rights reserved

Spanning Tree Configuration

Things To Consider

- **Draw the physical network topology**
  - If there is a loop anywhere, some links will get blocked
- **You must remove all VLANs associated with the STP before deleting the STPD**
  - If you delete an STPD, it will delete its member VLANs!!!
- **"S0" is a pre-configured STPD**
- **STPD are blind to VLAN membership**
- **STP, load-sharing and redundant physical port/link will work together.**
- **All STP parameters default to IEEE 802.1D values as appropriate**

Notes:

Things to Remember - VLANs and STP

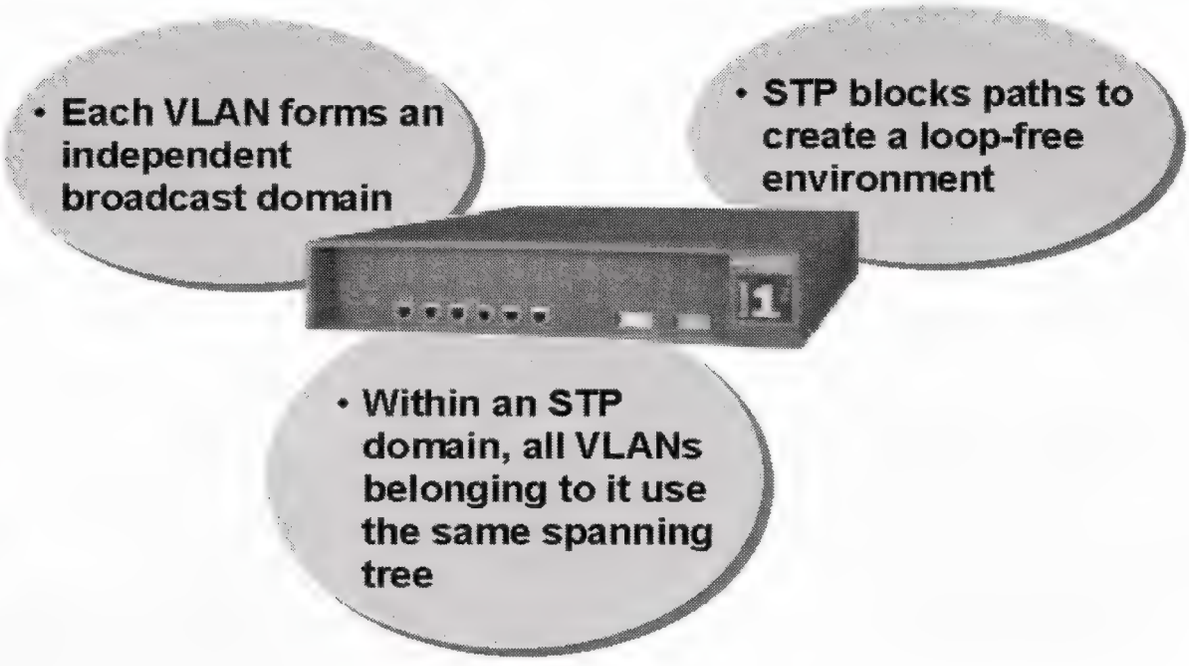
The key points to remember when configuring VLANs and STP are the following:

- Each VLAN forms an independent broadcast domain
- STP blocks path to create a loop-free environment
- When STP blocks a path, no data can be transmitted or received on the blocked port
- Within any given STPD, all VLANs belonging to it use the same spanning tree
- When assigning VLANs to an STPD, pay careful attention to the STP configuration and its effect on the forwarding of VLAN traffic

© 2001 Extreme Networks,Inc. All rights reserved

Things To Remember

VLANs and STP


• Each VLAN forms an independent broadcast domain
• STP blocks paths to create a loop-free environment
• Within an STP domain, all VLANs belonging to it use the same spanning tree

Notes:

Configuring STP - CLI Commands - 1

To configure STP, you must perform the following actions:

- Create one or more uniquely named STP domains

  (NOTE: STPD, VLAN and QoS profile names must all be unique. For example, a name used to identify a VLAN cannot be used when you create an STPD or a QoS profile)

- Add one or more VLANs to the STPD

- Enable STP for one or more STP domains

  (Once you have created STPDs, you can optionally configure STP parameters for each STPD based on your particular network needs)

NOTE: You should not modify STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

NOTE: The switch supports the RFC 1493 Bridge MIB. Parameters of only the s0 default STPD are accessible through this MIB.

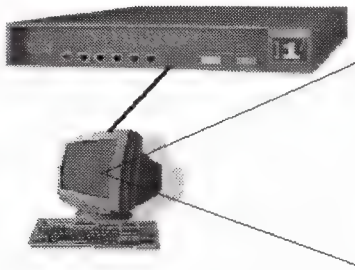
CLI Command – create STPD
create stpd <stpd_name>
Creates an STPD with the default parameters.

CLI Command – enable STPD
enable stpd {<stpd_name>}
Enables the STP protocol for one or all STPDs.

CLI Command – enable STPD ports
enable stpd <stpd_name> ports {<portlist>}
Enables the STP protocol on one or more ports.

© 2001 Extreme Networks,Inc. All rights reserved

Configuring STP - CLI Commands - 1



```
create stpd <stpd_name>
delete stpd <stpd_name>
enable stpd {<stpd_name>}
disable stpd {<stpd_name>}
enable stpd <stpd_name>ports {<portlist>}
disable stpd <stpd_name>ports{<portlist>}
```

Notes:

Configuring STP - CLI Commands - 2

The parameters that can be configured per STPD are:

- Hello time
- Forward delay
- Max Age
- Bridge Priority

The parameters that can be configured per port are:

- Path cost
- Port priority

CLI Command – add VLAN
config stpd <stpd_name> add vlan <vlan name>
Adds a VLAN to the spanning tree protocol domain.

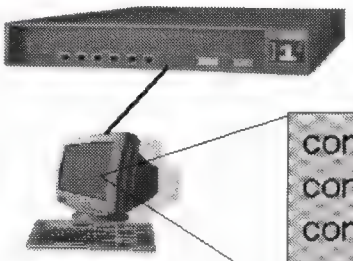
CLI Command – config priority
config stpd <stpd_name> priority <priority>
Specifies the bridge priority in the spanning tree protocol domain. By changing the priority, the bridge can be configured to be elected as the root bridge.

CLI Command – config port cost
config stpd <stpd_name> ports cost <cost> <portlist>
Specifies the path cost of the port in this spanning tree protocol domain.

CLI Command – ports priority
config stpd {<stpd_name>} ports priority <priority> <portlist>
Specifies the priority of the port in this spanning tree protocol domain. By changing the priority of the port, you can make it become the root port.

© 2001 Extreme Networks,Inc. All rights reserved

Configuring STP - CLI Commands - 2



```
config stpd <stpd_name>add vlan <vlan name>
config stpd <stpd_name>priority<priority>
config stpd <stpd_name>ports cost<cost><portlist>
config stpd {<stpd_name>}ports priority<priority><portlist>
```

Notes:

Configuring STP - CLI Commands - 3

CLI Command – hello timer
config stpd <stpd_name> hellotime <seconds>
Specifies the time delay (in seconds) between the transmission of BPDUs from this STPD when it is the Root Bridge.

CLI Command – forwarding delay timer
config stpd <stpd_name> forwarddelay <seconds>
Specifies the time (in seconds) that the ports in this STPD spend in the listening and learning states when the switch is the Root Bridge.

CLI Command – maximum age timer
config stpd <stpd_name> maxage <seconds>
Specifies the maximum age of a BPDU in this spanning tree protocol domain.

CLI Command – restore default STPD values
unconfig stpd {<stpd_name>}
Restores default spanning tree protocol values to a particular STPD or to all STPDs.

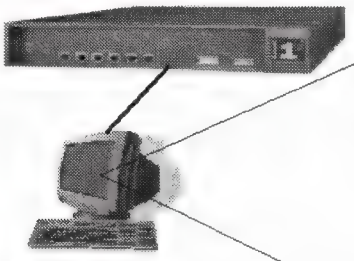
CLI Command – show STP settings
show stpd {<stpd_name>}
Displays the settings for this spanning tree protocol.

CLI Command – show stp port status
show stpd ports [all |<portlist>]
Displays the state of a spanning tree port.

CLI Command – ignore spanning tree
enable ignore-stp vlan <vlan_name>
Configures the switch to ignore the STP protocol, and not block traffic for the VLAN(s). This command is useful when multiple VLANs share the same physical ports, but only some of the VLANs require STP protection.

© 2001 Extreme Networks,Inc. All rights reserved

Configuring STP - CLI Commands - 3



```
config stpd <stpd_name>hellotime<seconds>
config stpd <stpd_name>forwardday<seconds>
config stpd {<stpd_name>}maxage<seconds>
Unconfig stpd{<stpd_name>}
Show stpd{<stpd_name>}
Show stpd<stpd_name>ports[all|<portlist>]
Enable ignore-stp vlan <vlan_name>
```

Notes:

CLI Command - show stpd

The CLI command "show stpd" displays spanning tree protocol information for one or for all spanning tree protocol domains.

The CLI command "show stpd" displays the following information:

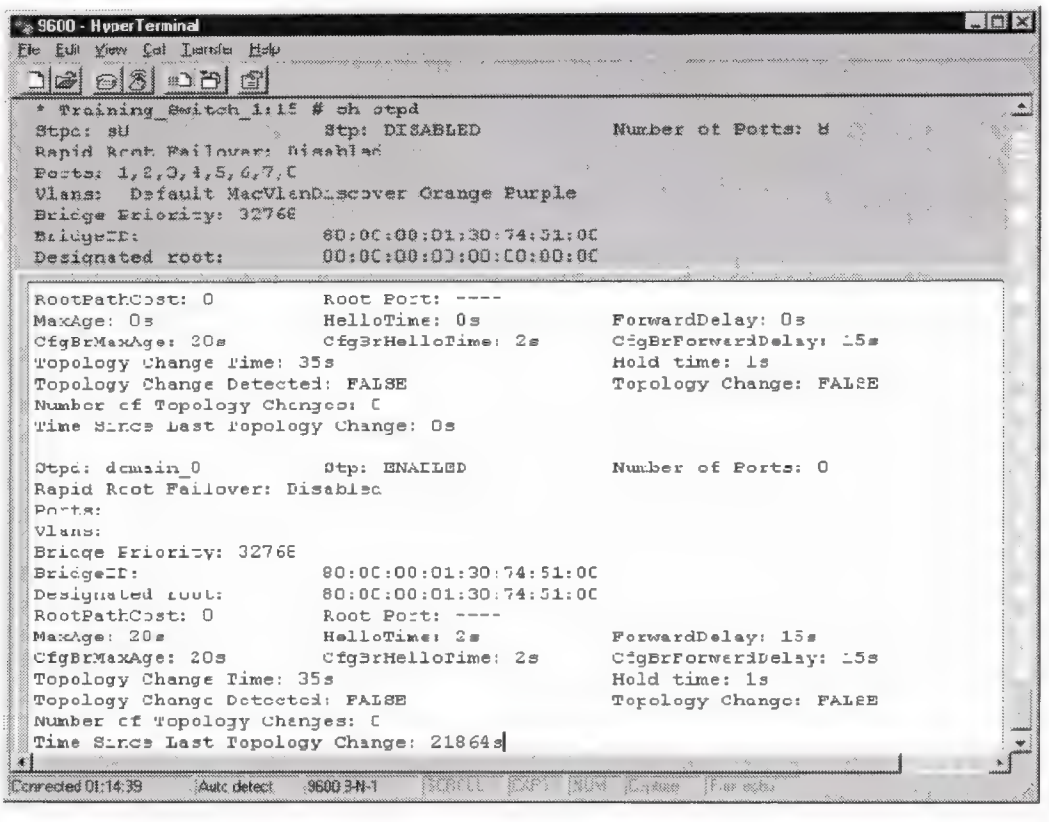
- STPD name
- Bridge ID
- STPD configuration information

NOTE: If the Bridge ID and the Designated Root matches, then this switch is the root bridge.

© 2001 Extreme Networks,Inc. All rights reserved

CLI Command

show stpd


9600 - HyperTerminal
File Edit View Call Transfer Help
* Training_Switch_1:15 # sh stpd
Stpd: s0 Stp: DISABLED Number of Ports: 8
Rapid Root Failover: Disabled
Ports: 1,2,3,4,5,6,7,8
Vlans: Default MacVlanDiscover Orange Purple
Bridge Priority: 32768
BridgeID: 80:0C:00:01:30:74:51:0C
Designated root: 00:0C:00:03:00:C0:00:0C
RootPathCost: 0 Root Port: ----
MaxAge: 0s HelloTime: 0s ForwardDelay: 0s
CfgBrMaxAge: 20s CfgBrHelloTime: 2s CfgBrForwardDelay: 15s
Topology Change Time: 35s Hold time: 1s
Topology Change Detected: FALSE Topology Change: FALSE
Number of Topology Changes: 0
Time Since Last Topology Change: 0s
Stpd: domain_0 Stp: ENABLED Number of Ports: 0
Rapid Root Failover: Disabled
Ports:
Vlans:
Bridge Priority: 32768
BridgeID: 80:0C:00:01:30:74:51:0C
Designated root: 80:0C:00:01:30:74:51:0C
RootPathCost: 0 Root Port: ----
MaxAge: 20s HelloTime: 2s ForwardDelay: 15s
CfgBrMaxAge: 20s CfgBrHelloTime: 2s CfgBrForwardDelay: 15s
Topology Change Time: 35s Hold time: 1s
Topology Change Detected: FALSE Topology Change: FALSE
Number of Topology Changes: 0
Time Since Last Topology Change: 21864s
Connected 01:14:39
Auto detect
9600 8-N-1

Notes:

CLI Command - show stpd port

The CLI Command "show stpd ports [all |<portlist>]" displays the status of a spanning tree port.

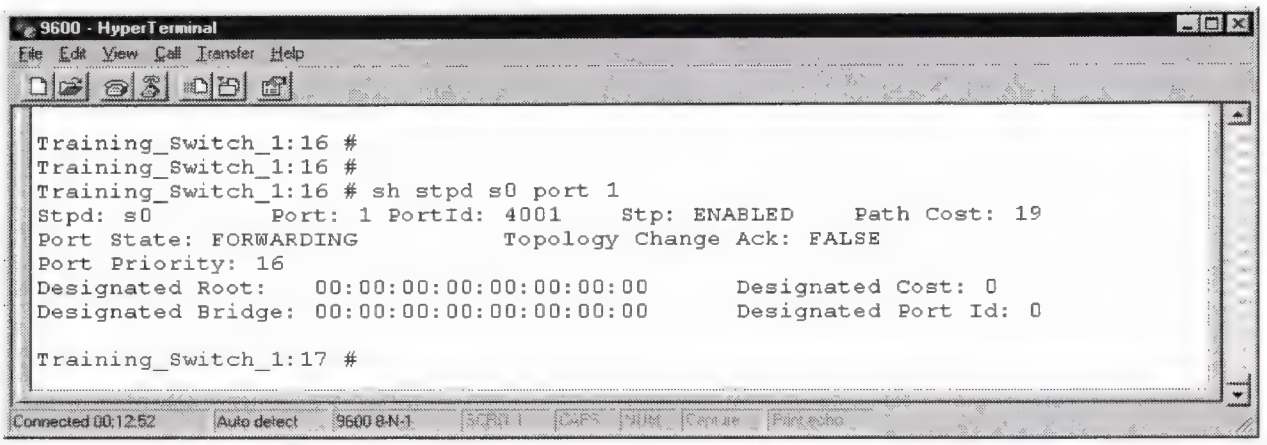
The CLI command "show stpd ports [all |<portlist>]" displays the following information:

- STPD port configuration
- STPD state (the Root Bridge etc.)
- STPD port state (forwarding and blocking etc.)

© 2001 Extreme Networks,Inc. All rights reserved

CLI Command

show stpd port


9600 - HyperTerminal
File Edit View Call Transfer Help
Training_Switch_1:16 #
Training_Switch_1:16 #
Training_Switch_1:16 # sh stpd s0 port 1
Stpd: s0 Port: 1 PortId: 4001 Stp: ENABLED Path Cost: 19
Port State: FORWARDING Topology Change Ack: FALSE
Port Priority: 16
Designated Root: 00:00:00:00:00:00:00:00 Designated Cost: 0
Designated Bridge: 00:00:00:00:00:00:00:00 Designated Port Id: 0
Training_Switch_1:17 #
Connected 00:12:52
Auto detect
9600 8-N-1

Notes:

Summary

Chapter seven has studied the IEEE 802.1D Spanning Tree Algorithm and Protocol, and examined the implementation of the spanning tree protocol on traditional bridge technology. This chapter has also provided you with an explanation of how the spanning tree protocol may be configured on the Extreme Networks switch product family. You should now be able to:

- Define the spanning tree protocol in an overview
- Explain how spanning tree works
- Determine the building blocks of STP
- Describe ports, VLANs, and the STPD relationship
- Configure STP on an Extreme Networks switch
- Successfully complete the lab exercises on STP configuration

© 2001 Extreme Networks,Inc. All rights reserved

Summary

You should now be able to:

- **Define Spanning Tree Protocol in an overview**
- **Explain how Spanning Tree works**
- **Determine the building blocks of STP**
- **Describe Ports, VLANs, STPD relationship**
- **Describe how to configure STP on an Extreme Networks Switch**
- **Successfully complete the lab exercises on STP configuration**

Notes:

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 8

IP Unicast Routing and Configuration

Chapter Objectives

The main theme of chapter eight is to discuss the Layer 3 unicast routing fundamentals, primarily IP forwarding, IP routing functionality and configuration available on the Extreme Networks range of switches.

Upon completion of this chapter, you will be able to:

- Describe Layer 3 Operations and differentiate between IP forwarding and Routing Functions
- Discuss ExtremeWare supported IP features
- Define RIF, IP Route Tables and IPFDB
- Describe how to populate entries in the IPFDB and IP Route Table
- Configure IP Unicast Routing

Successfully complete lab exercises

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

Upon completion of this chapter, you will be able to:

- **Describe Layer 3 Operations and differentiate between IP forwarding and Routing Function**
- **Discuss ExtremeWare supported IP features**
- **Define RIF, IP Route Tables and IPFDB**
- **Describe how to populate entries in the IPFDB and IP Route Table**
- **Configure IP Unicast Routing**
- **Successfully complete lab exercises**

Notes:

How Routing is Accomplished

The Extreme Forwarding function has two components:

- For unknown destinations, the forwarding decisions are made by the CPU.
- For learned host addresses, layer-3 switching performs hardware lookups of an IP forwarding database and makes forwarding decisions based on the results.

The Extreme Networks family of enterprise LAN switches deliver both Layer 2 and Layer 3 switching. Layer 3 switching is essentially very fast routing. Extreme Networks is able to route IP traffic at wire speed on all switch ports. This is true routing that utilises industry-standard routing protocols.

Extreme Networks switches, because they perform true routing, will inter-operate with existing legacy routers on a network. As a result, the network manager can configure large meshed topologies that offer increased fault tolerance and redundancy.

Very large networks can be built by combining wire-speed Layer 2 and Layer 3 switching, enabling a logical partitioning of users and groups on top of a high-performance switched infrastructure.

IP Forwarding Configuration

Wire-speed IP routing enables you to route where you can and only switch where you must - i.e. you can select Layer 3 functions wherever possible and only use Layer 2 functionality where Layer 3 won't work (non-routing protocol support). The robustness and redundancy of Layer 3 can be used rather than having to rely on Layer 2.

CLI Command – Enable/disable ipforwarding

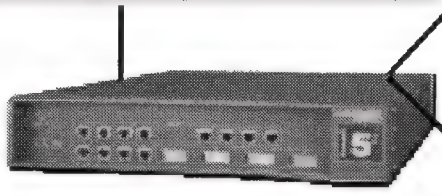
enable ipforwarding {vlan <name>}
disable ipforwarding {vlan <name>}
Enables/disables IP routing for one or more VLANs. If no argument is provided, it will enable routing for all VLANs that have been configured with an IP address.

NOTE: A common error found during configuration is after configuring the VLANs routing does not appear to work. This is because IP Forwarding is not enabled on the VLANs created. IP Forwarding will need to be enabled on every VLAN created.

© 2001 Extreme Networks,Inc. All rights reserved

How Routing Is Accomplished

- **IP Forwarding function is disabled by default**



- **The switch will not be able to route until:**
  - IP forwarding is enabled
  - VLAN is assigned an IP address
  - VLAN is configured to use a routing protocol or static routes
  - The routing protocol is enabled globally on the switch

- **The Extreme Networks switch forwarding function has two components:**
  - For unknown destinations forwarding decisions are made by the CPU
  - For learned host addresses, layer 3 switching performs hardware lookups of IP forwarding database

Notes:

Layer 2 Operations Review

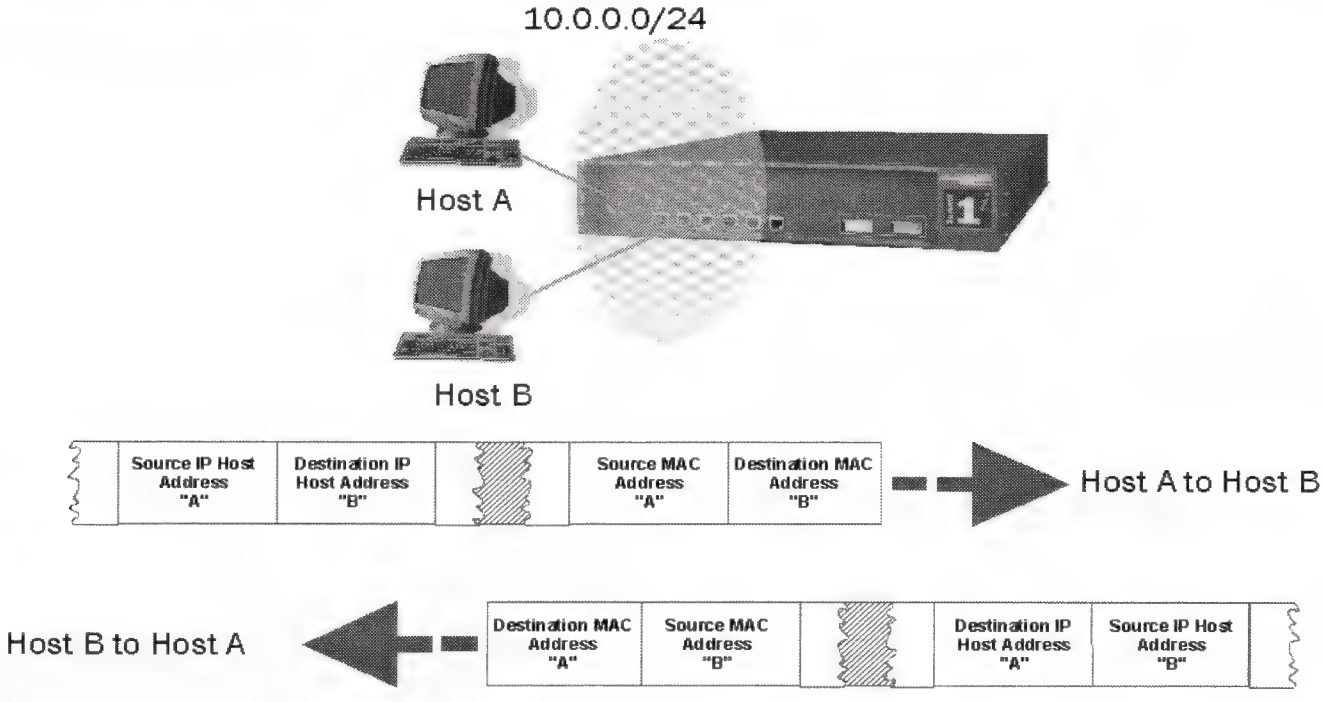
When performing IP forwarding within the same VLAN, end-stations have to resolve the Layer 3 destination address to the destination MAC address.

If Host A wishes to send an IP packet to Host B, Host A will have to determine Host B's layer 2 address. This is accomplished using the Address Resolution Protocol (ARP). Host A will send a broadcast ARP message asking all devices in the broadcast domain if they are configured with the target IP address. Host B should reply with an ARP response containing Host B's MAC address. This will enable Host A to build a frame to send the IP packet to Host B.

When the switch sees a destination MAC address that is not its own, the switch knows that this is a Layer 2 function. Therefore, the switch will act as a layer 2 bridge and will perform a Layer 2 forwarding function by doing a lookup on the Forwarding Database. When the switch sees a destination MAC address which is its own, it knows to perform Layer 3 forwarding.

© 2001 Extreme Networks,Inc. All rights reserved

Layer-2 Operations Review



Each host will use ARP to resolve the layer 2 destination address

Notes:

Layer 3 Operations - IP Forwarding Function

When forwarding an IP packet between two subnets (VLANs) on the same switch, the source host can see from the destination IP address that the target host is on a different subnet and will need to forward the packet to the default gateway.

The source host will use ARP to resolve the layer 2 address of the gateway (in this case the VLAN's router interface of the switch). Once the switch has received the packet it needs to make a decision as to which interface to use in order to forward the packet.

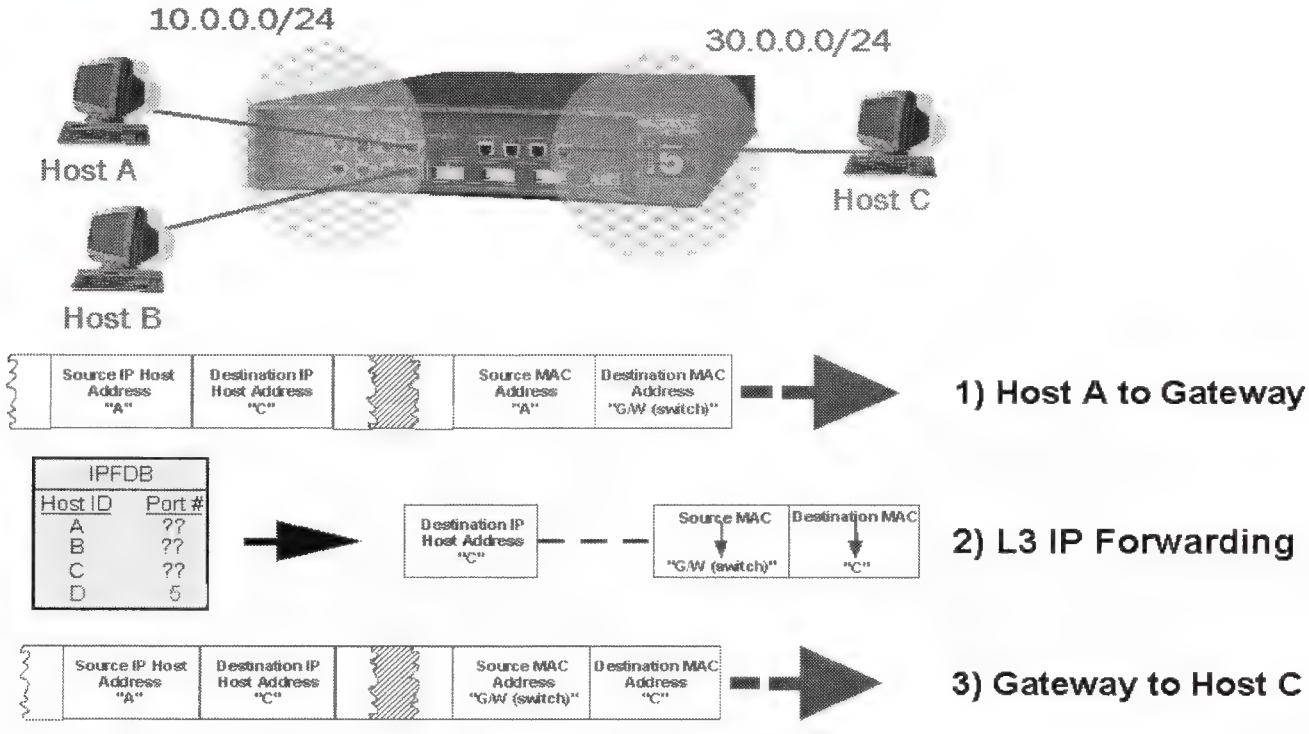
The forwarding decision will be made by the Switch ASIC consulting the IPFDB. The IPFDB already has this information because all of the networks are directly attached to the switch.

Once the decision is made, the switch will ARP the destination host to resolve the layer 2 address so it can forward the packet to it's destination and make an entry in the IPFDB.

© 2001 Extreme Networks,Inc. All rights reserved

Layer-3 Operations

IP Forwarding Function



Notes:

Layer 3 Operations - IP Routing

The Layer 3 routing capability is used to facilitate communication between devices in different broadcast domains (VLANs).

The switch's routing process consults a table that tells the router where to forward the packets. This routing table is simply a collection of all known networks and the local interface used to reach them. It is used to match the destination address to a network.

When it is time to do a lookup of an unknown IP destination host address, the protocol's function is to learn the route to take by comparing the destination address to the list of networks in the routing table.

In a traditional router the forwarding decision will be made by the CPU consulting the Route Table to find the destination network and the interface on which to forward the IP packet. In a traditionally routed network this action is performed for every packet at every router hop between source and destination. In an Extreme Networks switch, performing IP forwarding at wire speed, the routing decision needs to be made in hardware and an IP forwarding Database is used to perform this function. The routing function works in the same way but is performed only once (for the first packet). An entry can then be made in the IPFDB and IP forwarding for all other packets will be done at wire speed.

Within a single switch, communication between two or more directly connected networks is enabled through the IP forwarding Database (IPFDB).

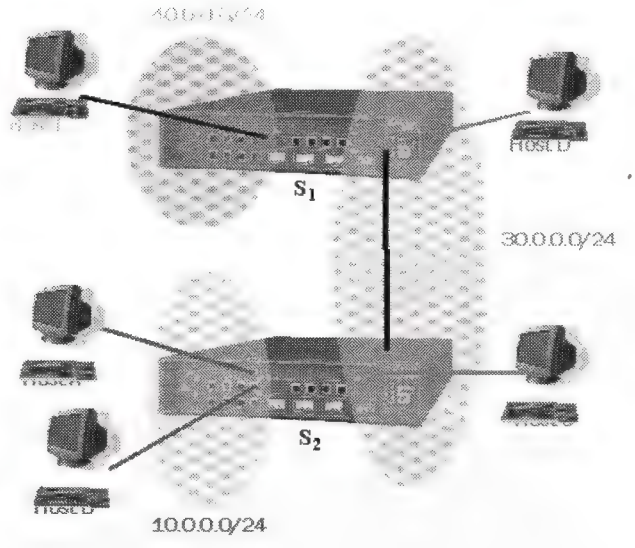
Between switches across a network, packets are moved over multiple boundaries using information in the IPFDB, if however, the destination network is unknown by the IPFDB then the CPU consults the Route Table for the first packet.Once this information has been learned the CPU can populate the IPFDB so that any other packets to this destination network can be forwarded at wire speed.

The slide shows each switch with a route table configured with all of the reachable networks. If the destination network 40.0.0.0/24 cannot be seen in the IPFDB of switch 2, the CPU of switch 2 will have to consult the route table to make its forwarding decision.

© 2001 Extreme Networks,Inc. All rights reserved

Layer 3 Operations - IP Routing

Spanning Multiple Switches



Network Table for Switch 1

Destination Network	Network Gateway	Metric
30.0.0.0/24	30.0.0.S_1 /24	1
40.0.0.0/24	40.0.0.S_1 /24	1
10.0.0.0/24	30.0.0.S_2/24	2

Network Table for Switch 2

Destination Network	Network Gateway	Metric
10.0.0.0/24	10.0.0.S_2 /24	1
30.0.0.0/24	30.0.0.S_2 /24	1
40.0.0.0/24	30.0.0.S_1 /24	2

Notes:

The IPFDB and IP Route Table

The switch uses tables to determine the destination for a received packet, for example at Layer 2, the FDB is a table of MAC layer information. There is also the IPARP table that is used to cache the mapping of MAC addresses and IP addresses the switch has been able to reach.

The CLI command "show iparp" will display the Address Resolution Protocol (ARP) table. The display can be filtered by IP address, VLAN or permanent entries.

When the destination IP address is unknown, the switch uses the following hierarchy to do IP forwarding and/or IP routing.

IP Forwarding Database – IPFDB
This is the ASIC's look-up table containing IP host routes and its outbound VLAN interface and port. It can hold 32,000 IP host routes and is populated only by the CPU.

IP Route Table
This is maintained by the CPU and is used to make forwarding decisions for unknown IP hos addresses (address not found in the IPFDB).
In the scenario shown, Host D wants to talk to Host B, and Host B is reachable via the switch:

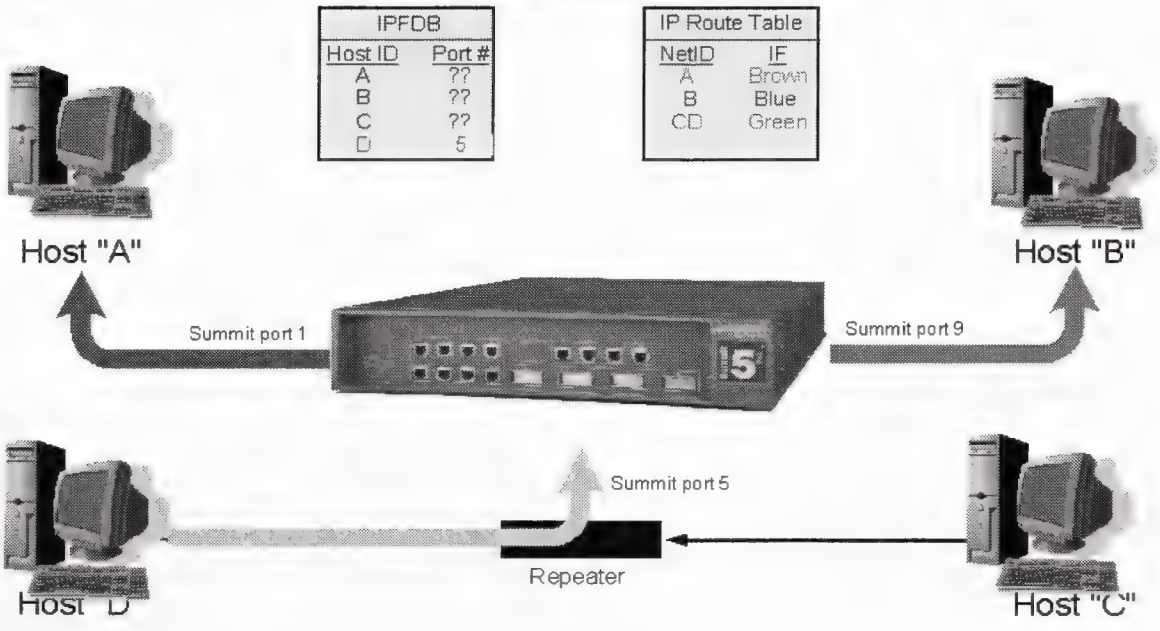
- When the destination MAC address is the switch, then it is determined that the switch is being asked to perform a layer 3 function.
- The ASIC tries to match the destination IP host address of the packet with the IPFDB. The ASIC uses the IPFDB for lookups, and only the CPU uses the routing table for lookup.
- When the ASIC finds that there is no match in the IPFDB, the packet is passed to the CPU.
- The CPU matches the destination IP address with the IP route table and forwards out the associated interface.
- It puts the IP host address into the IPFDB as a host entry
- It then checks the source IP host address and adds it to the IPFDB.

Remember, the IPFDB is populated with Layer-3 information. With Layer 3 switching, we learn the source and destination in one pass.

© 2001 Extreme Networks,Inc. All rights reserved

The IPFDB and IP Route Table

- **At the same time, the CPU extracts the source IP address and adds it to the IP forwarding database**



Notes:

Displaying IPFDB

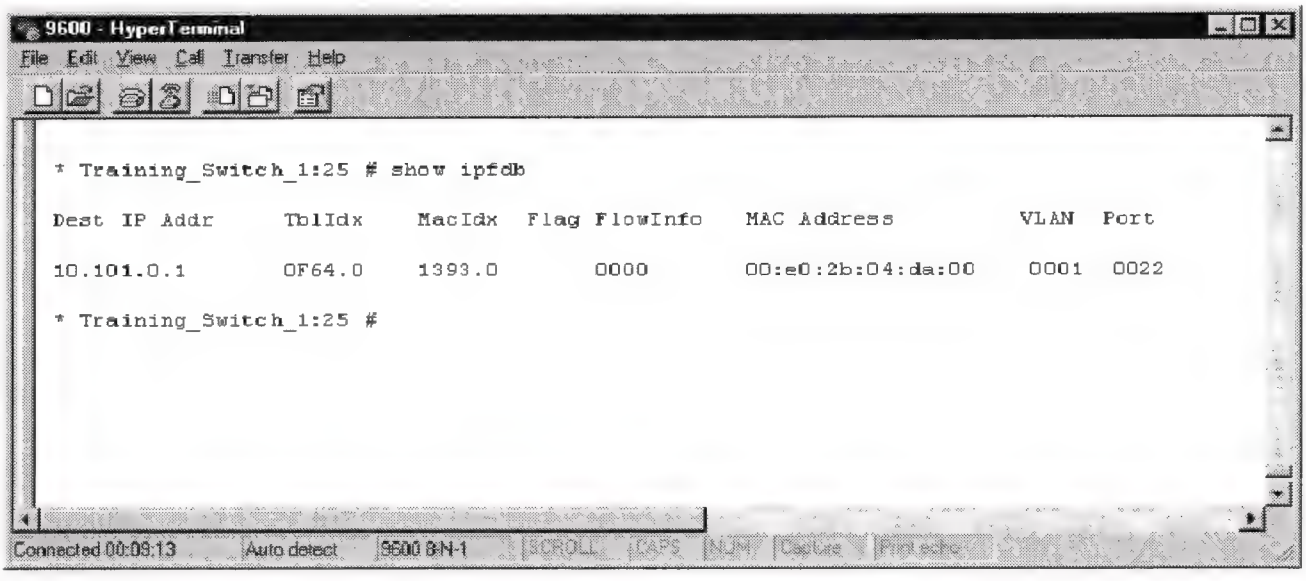
CLI Command – Show ipfdb

show ipfdb { vlan <vlan name> | <ip address> }

Displays the host entries that have been transmitting or receiving packets, and the port and VLAN for each host entry.

© 2001 Extreme Networks,Inc. All rights reserved

Displaying IPFDB



Notes:

Router Interface - (RIF)

The Layer 3 software and hardware function forwards IP traffic between router interfaces for inter-VLAN communication. IP Forwarding will need to be enabled on the VLAN so the switch can recognise that it is to perform a Layer 3 function.

In order to participate in routing, a VLAN must have an IP address assigned to it this is called a Router Interface.

As you create VLANs with IP addresses belonging to different IP subnets, you can also choose to forward between the VLANs. Both the MAC switching and IP forwarding function occur within the switch (meaning both Layer 2 and Layer 3 functions occur within the switch).

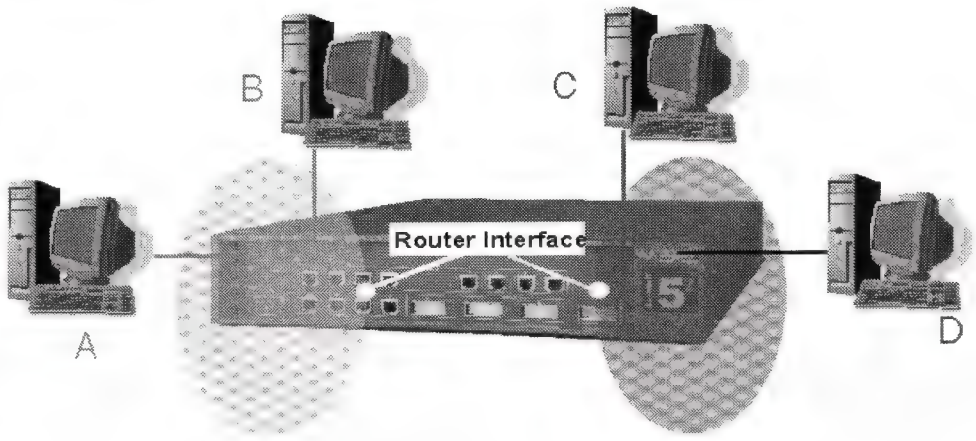
The router interface IP address and mask assigned to the VLAN must represent a unique IP subnet. You cannot configure the same IP subnet on different VLANs.

The example shows a Summit5i with two VLANs defined: Green and Purple. Green belongs to network 192.206.35.0 and the router interface (VLAN) for Green is assigned the IP address o 192.206.35.1. Purple belongs to the IP network 192.207.36.0 and the router interface (VLAN) for Purple is assigned the IP address of 192.207.36.1. Traffic between the two VLANs is forwarded based on the configured network information (IP address and mask).

© 2001 Extreme Networks,Inc. All rights reserved

Router Interface - (RIF)

- **Simply a VLAN configured with an IP Address**



Network: 192.206.35.0/24 Network: 192.207.36.0/24

VLAN Green : 192.206.35.1/24 VLAN Purple: 192.207.36.1 /24

Notes:

IP Route Table Entries

The switch maintains an IP routing table for both network and host routes. The table is populated either dynamically or statically.

There are several types of IP route table entries:

- Directly-connected networks
- When configured will always be in the IP route table
- Dynamic route entries
- Permanent routes

Permanent routes are statically configured routes and can be further categorised as:

- Static
- Blackhole
- Default

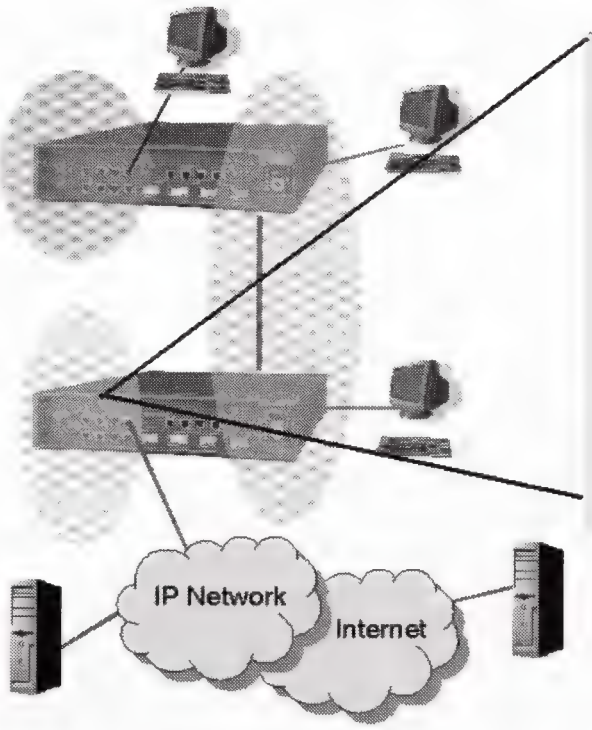
If you define a default route, and subsequently delete the VLAN on the subnet associated with the default route, the invalid default route entry remains. You must manually delete the configured default route.

Default gateway -
change something in to something out

Default route -
send something, don't know. please send others to figure out
know. please send it

© 2001 Extreme Networks,Inc. All rights reserved

IP Route Table Entries



- The routing table contains entries on how to get to required destinations
- The type of entries may be:
  - Dynamically learned route entries
  - Manually configured route entries:
    - Static Routes
    - Blackhole Routes
    - Default Routes
- The routing table may also contain multiple entries for a destinaton

Notes:

Dynamic Route Entries

Dynamic route table entries are reachable routes learned via a dynamic routing protocol such as RIP, OSPF or BGPv4.

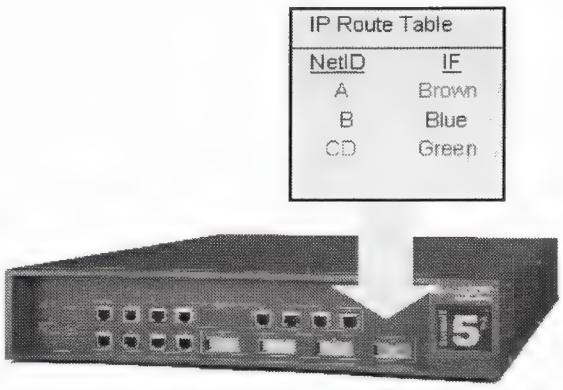
The maximum number of entries possible varies depending on which routing protocol is used:

- RIP - 8,000
- OSPF - 30,000 (Summit1i, 5i, 48i) 100,000 (BlackDiamond, Alpine and Summit 7i)
- BGP - 250,000 (Summit1i, 5i, 48i) or 1,000,000 (BlackDiamond, Alpine and Summit 7i)

Dynamic entries are aged out when an update is not received for a period of time. This is a function of the routing protocol used.

© 2001 Extreme Networks,Inc. All rights reserved

Dynamic Route Entries



- **Reachable routes learned via RIP, OSPF or BGP**
- **Holds learned routes based on the protocol:**
  - RIP - 8,000
  - OSPF - 30,000 (Summit1i, 5i, 48i) 100,000 (BlackDiamond, Alpine and Summit 7i)
  - BGP - 250,000 (Summit1i, 5i, 48i) or 1,000,000 (BlackDiamond, Alpine and Summit 7i)
- **Are aged out when an update is not received for a period of time based on the routing protocol**

keep the routing table updated by "aged out"

Notes:

Permanent Routes - Static and Blackhole

Static Routes

Static routes are permanent routes manually entered into the routing table. They are used to reach networks not normally advertised by dynamic routing protocols. Static routes are never aged out of the routing table.

Up to 1024 static routes can be configured on Extreme Networks switches.
Static routes can be used for security reasons, to control which routes you want advertised by the router.

CLI Command – Enable Static Route Advertisements

[enable | disable] rip export static
[enable | disable] ospf export static
Advertises all static routes via RIP or OSPF.
A static route must be associated with a valid IP subnet. An IP subnet is associated with a single VLAN by its IP address and subnet mask. If the VLAN is subsequently deleted, the static route entries using that subnet must be deleted manually.

CLI Command – Add Static Route

configure iproute add <ipaddress> / <netmask> <gateway> <metric>
Adds a static route.

Blackhole Routes

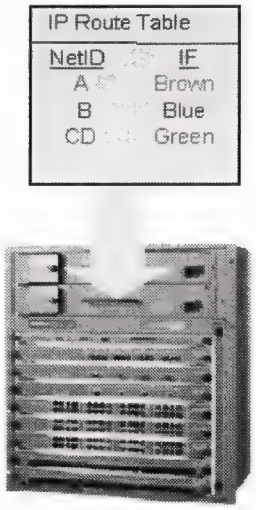
Blackhole routes are permanent routes, configured to enable traffic to specific destinations to be dropped. These are treated like permanent entries in the event of a switch reset or power off/on cycle, and are never aged out of the routing table.
Blackhole routes will be configured as an entry in the IP Route table with a specific IP destination address. When a packet is received with destination address matching a blackhole route, the packet will be discarded. This type of route table entry is generally used as a security measure but can also be used in special circumstances where a specific destination address must be discarded.

CLI Command – Add Blackhole Route

configure iproute add blackhole <ipaddress> / <netmask>
Configures a blackhole route.

© 2001 Extreme Networks,Inc. All rights reserved

Permanent Routes
Static and Blackhole



- **Static Routes**
  - Manually entered
  - Used to reach networks not advertised by routers
  - Maximum 1024 static routes
  - Never aged out of the routing table (no timeout)
- **Blackhole Routes**
  - Configured into the IP route table with a specified IP destination address
  - Used as a security measure
  - Never aged out of the routing table

Notes:

Multiple Entries in the Route Table

Multiple entries can be placed in a route table this may be used for the purposes of redundancy. When there are multiple, conflicting choices of a route to a particular destination, the router picks the route with the longest matching network mask.

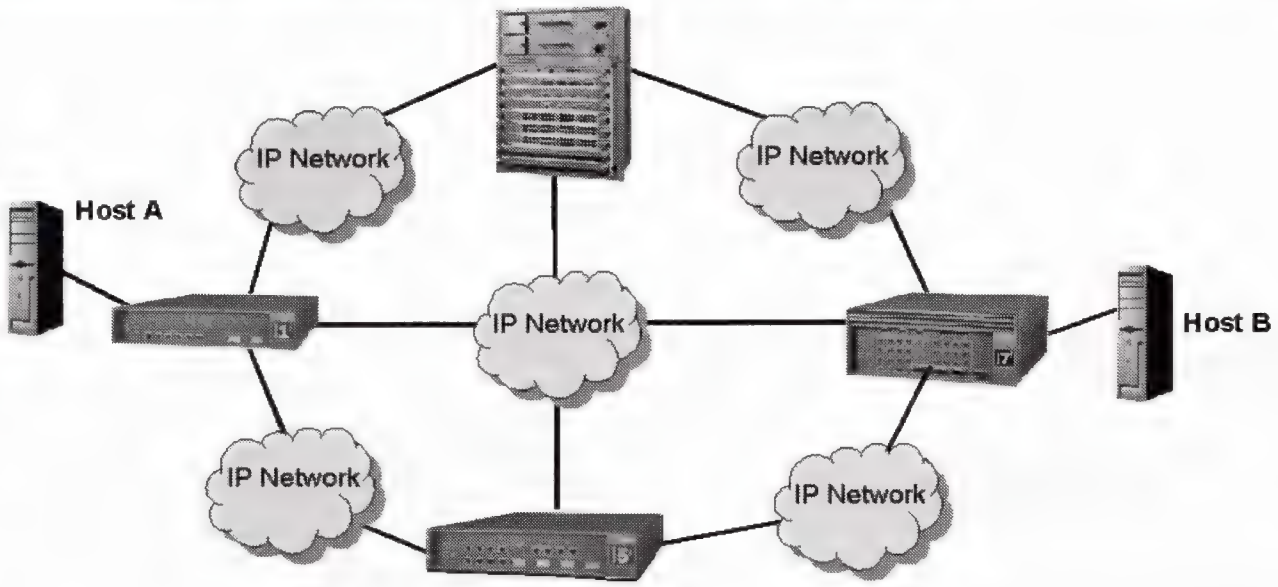
If these are still equal, the router picks the route using the following criteria (in the order specified):

- Directly attached network interfaces
- Static routes
- ICMP redirects

NOTE: If you define multiple default routes, the route that has the lowest metric is used. If there are multiple default routes that have the same lowest metric, the system picks the first one in the routing table

© 2001 Extreme Networks,Inc. All rights reserved

Multiple Entries in the Route Table



- The route tables for the switches may show multiple routes to reach each destination

Notes:

Relative Route Priorities

Relative route priorities will be assigned to routes learned by the switch depending upon the source of the routing information. The table shown lists the relative priorities assigned to different routing protocol sources. Directly connected networks will always get the highest priority.

CLI Command – Change IP Route Priority

config iproute priority [bootp | e-bgp | i-bgp | icmp | ospf-extern1 | ospf-extern2 | ospf-inter | ospf-intra | rip | static] <priority>

Changes the priority for all routes from a particular routing information origin.

NOTE: Do not attempt any manipulation unless you are expertly familiar with the possible consequences.

IP Route Sharing

IP route sharing allows multiple equal-cost routes to be used concurrently. Some protocols may only use one route even when multiple routes of the same metric exist. IP route sharing can be used with static routes or with OSPF routes. In OSPF, this capability is referred to as equal cost multi-path (ECMP) routing.

To use IP route sharing, first enable it, then configure static routes and/or OSPF as you would normally. As many as eight ECMP routes can be used for a given destination.

Route sharing is useful only in instances where you are constrained for bandwidth. This is typically not the case using Extreme Networks switches. Using route sharing makes router troubleshooting more difficult because of the complexity in predicting the path over which the traffic will travel.

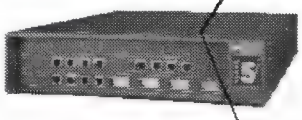
CLI Command – Enable IP Route Sharing

enable iproute sharing

Enables IP route sharing.

© 2001 Extreme Networks,Inc. All rights reserved

Relative Route Priorities



Route Origin	Route Priority
Direct	10
BlackHole	50
Static	1100
ICMP	1200
EBGP	1700
IBGP	1900
OSPF	2100
OSPFIntra	2200
OSPFInter	2300
RIP	2400
OSPFAsExt	3100
OSPFExt1	3200
OSPFExt2	3300
BOOTP	5000

Notes:

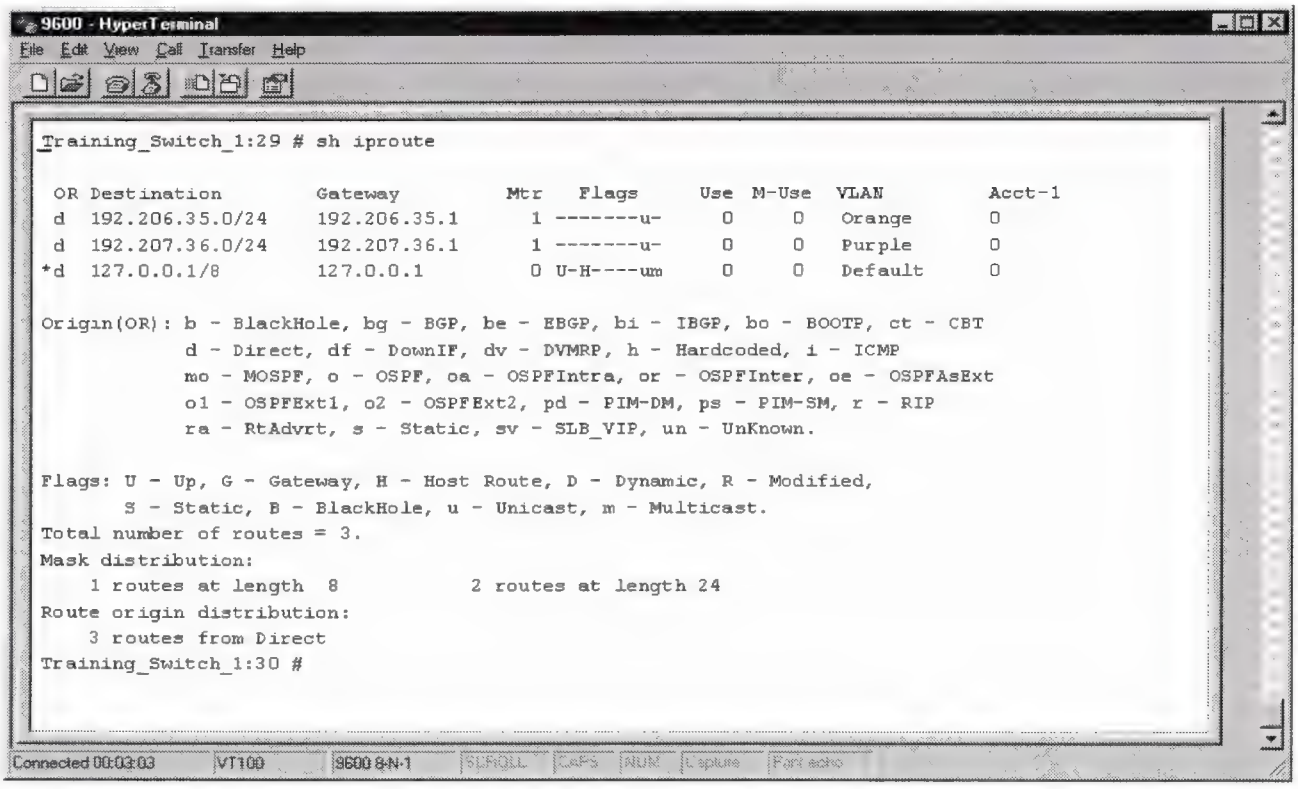
Displaying IP Route Table

CLI Command – Show IP Route

show iproute { origin [bgp | blackhole | direct | e-bgp | i-bgp | ospf-extern1 | ospf-extern2 | ospf-inter | ospf-intra | rip | static]
| permanent | priority | route-map | sorted | summary | vlan <vlan_name> | <ip address> }
Displays IP route table entries.

© 2001 Extreme Networks,Inc. All rights reserved

Displaying IP Route Table


9600 - HyperTerminal
File Edit View Call Transfer Help
Training_Switch_1:29 # sh iproute
OR Destination Gateway Mtr Flags Use M-Use VLAN Acct-1
d 192.206.35.0/24 192.206.35.1 1 -------u- 0 0 Orange 0
d 192.207.36.0/24 192.207.36.1 1 -------u- 0 0 Purple 0
*d 127.0.0.1/8 127.0.0.1 0 U-H----um 0 0 Default 0
Origin(OR): b - BlackHole, bg - BGP, be - EBGP, bi - IBGP, bo - BOOTP, ct - CBT
d - Direct, df - DownIF, dv - DVMRP, h - Hardcoded, i - ICMP
mo - MOSPF, o - OSPF, oa - OSPFIntra, or - OSPFInter, oe - OSPFAsExt
o1 - OSPFExt1, o2 - OSPFExt2, pd - PIM-DM, ps - PIM-SM, r - RIP
ra - RtAdvrt, s - Static, sv - SLB_VIP, un - UnKnown.
Flags: U - Up, G - Gateway, H - Host Route, D - Dynamic, R - Modified,
S - Static, B - BlackHole, u - Unicast, m - Multicast.
Total number of routes = 3.
Mask distribution:
1 routes at length 8
2 routes at length 24
Route origin distribution:
3 routes from Direct
Training_Switch_1:30 #
Connected 00:03:03
VT100
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Notes:

Other IP Unicast Features

Proxy ARP - Proxy Address Resolution Protocol

Proxy ARP allows the switch to answer ARP requests for other stations there are two cases where this is needed:

- Devices on a subnet are not capable of responding to an ARP request
- When a station cannot access a default gateway because it is configured with a more general subnet mask than that of the switch

IP Multinetting

In many legacy IP networks, there is a need to overlap multiple subnets into one physical port with third-party devices that do not support tagging. In normal operation, you can only assign a port untagged once to a router interface. IP multinetting allows untagged assignment of multiple VLANs to the same physical port.

DHCP/BOOTP Relay

This feature can be used in various applications, including DHCP services between Microso Windows NT servers and clients running Windows 95/98 etc.

UDP Forwarding

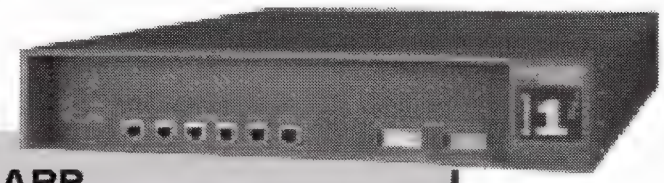
UDP forwarding is used to handle the directed forwarding of broadcast UDP packets. It allows applications to be directed to different DHCP servers. Example applications are multiple DHCP relay services from differing sets of VLANs.

VLAN Aggregation

A feature aimed primarily at Service Providers. It is used to increase the efficiency of IP address space usage by allowing clients within the same IP subnet to use different broadcast domains while still using the same default router.

© 2001 Extreme Networks,Inc. All rights reserved

Other IP Unicast Features



- Proxy ARP
- IP Multinetting
- DHCP/BOOTP relay
- UDP Forwarding
- VLAN Aggregation

- Refer to the ExtremeWare Software User Guide for more details

Notes:

Configuring IP Unicast Routing

Configuring routing on the Extreme Networks switch involves the following steps:

- Create and configure two or more VLANs
- Assign an IP address to each VLAN that will be using routing. Ensure that each VLAN has a unique IP address in a different subnet.
- Enable IP forwarding for one or all VLANs
- Add IP Forwarding-enabled VLANs to routing protocol
- Enable routing protocol (RIP or OSPF)

NOTE: Although it is possible to enable IP forwarding and an IP routing protocol (such as RIP) with only one VLAN defined, the switch does not route unless at least two VLANs are created and configured.

CLI Command – Create VLAN
create vlan <vlan_name>
Creates the VLAN on the switch.

CLI Command – Config VLAN
config <vlan_name> add ports [all | <port number>]
Adds the ports to the VLAN.

CLI Command – Config VLAN IP Address
config <vlan_name> ipaddress <ipaddress> [/<netmask>]
Adds the IP address to the VLAN.

CLI Command – Enable IP Forwarding
enable ipforwarding
Enables IP forwarding.

CLI Command – Add VLANs to Routing Protocol
config rip add vlan [all | <vlan_name>]
config ospf add vlan [all | <vlan_name>] area <area_identifier>
Adds the VLANs to the required routing protocol.

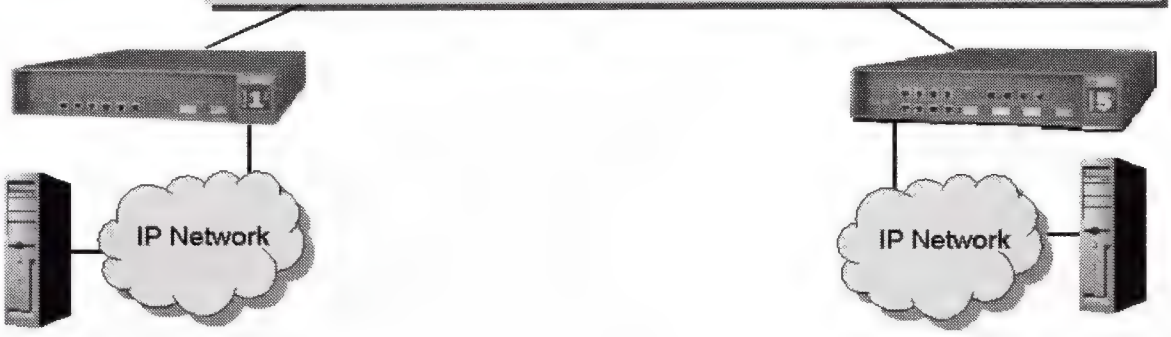
CLI Command – Enable Routing Protocol
enable <rip>
enable <ospf>
Enables the routing protocol.

© 2001 Extreme Networks,Inc. All rights reserved

Configuring IP Unicast Routing

point-to-point.

1 - Create and configure two or more VLANs
2 - Assign an IP address for two or more VLANs
3 - Enable IP forwarding for two or more VLANs
4 - Add IP Forwarding-enabled VLANs to routing protocol
5 - Enable routing protocol (RIP or OSPF)



Notes:

CLI Command – Add/Delete Static Address
config iproute add <ipaddress> / <netmask> <gateway> {<metric>}
config iproute delete <ipaddress> / <netmask> <gateway>
Adds or deletes a static address to the routing table. Use a value of 255.255.255.255 for mask to indicate a host entry.

CLI Command – Add/Delete Default Gateway
config iproute add default <gateway> {<metric>}
config iproute delete default <gateway>
Adds or deletes a default gateway to the routing table. A default gateway must be located on a configured IP interface.

CLI Command – Add/Delete Blackhole Address
config iproute add blackhole <ipaddress> / <netmask>
config iproute delete blackhole <ipaddress> / <netmask>
Adds or deletes a blackhole address to the routing table. All traffic destined for the configured IP address is dropped, and no Internet Control Message Protocol (ICMP) message is generated.

CLI Command – Clear iparp
clear iparp {vlan <vlan name>|<ipaddress>}
Removes dynamic entries from the IP ARP table. Permanent IP ARP entries are not affected.

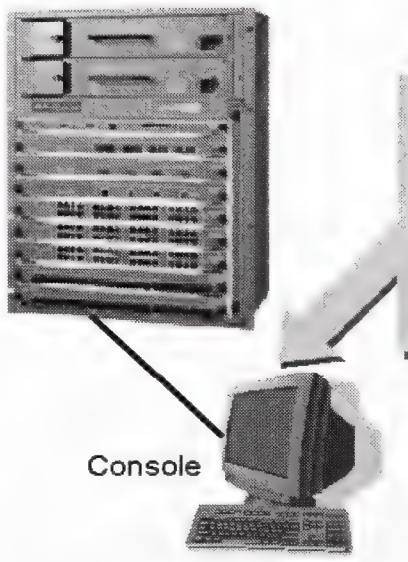
CLI Command – Clear ipfdb
clear ipfdb {vlan <vlan name>|<ipaddress>}
Removes the dynamic entries in the IP forwarding database.

CLI Command – Enable irdp
enable irdp {vlan <vlan name>}
Enables the generation of ICMP router advertisement messages on one or more VLANs.

CLI Command – Enable icmp unreachables
enable icmp unreachables vlan [all|<vlan name>]
disable icmp unreachables vlan [all|<vlan name>]
Enables or disables the generation of ICMP unreachable messages on one or more VLANs.

© 2001 Extreme Networks,Inc. All rights reserved

IP Routing - CLI Commands



- Add static entries in the IP route table
- Clear entries in the IPARP and IPFDB table
- Enable/disable ICMP messages
- Show commands

don't want others learn your network.

Notes:

Show ipconfig - Global Flags

The next three slides show an example display of a show ipconfig command (Version 6.1.8b12).

The display has been separated based on:

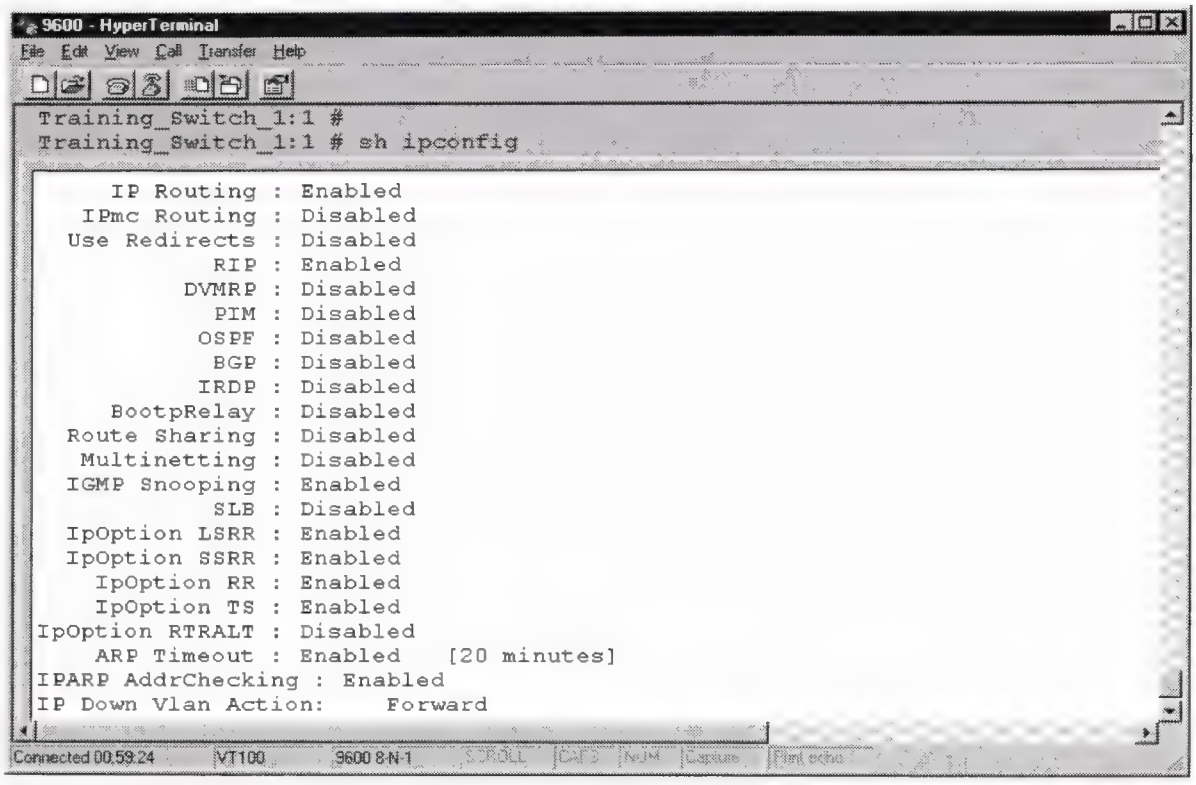
- Global Flags
- Global Timers
- VLAN specific Information

CLI command - show ipconfig
show ipconfig
Used to display the current configuration of IP unicast routing for the switch, and for each VLAN.

© 2001 Extreme Networks,Inc. All rights reserved

Show ipconfig

Global Flags



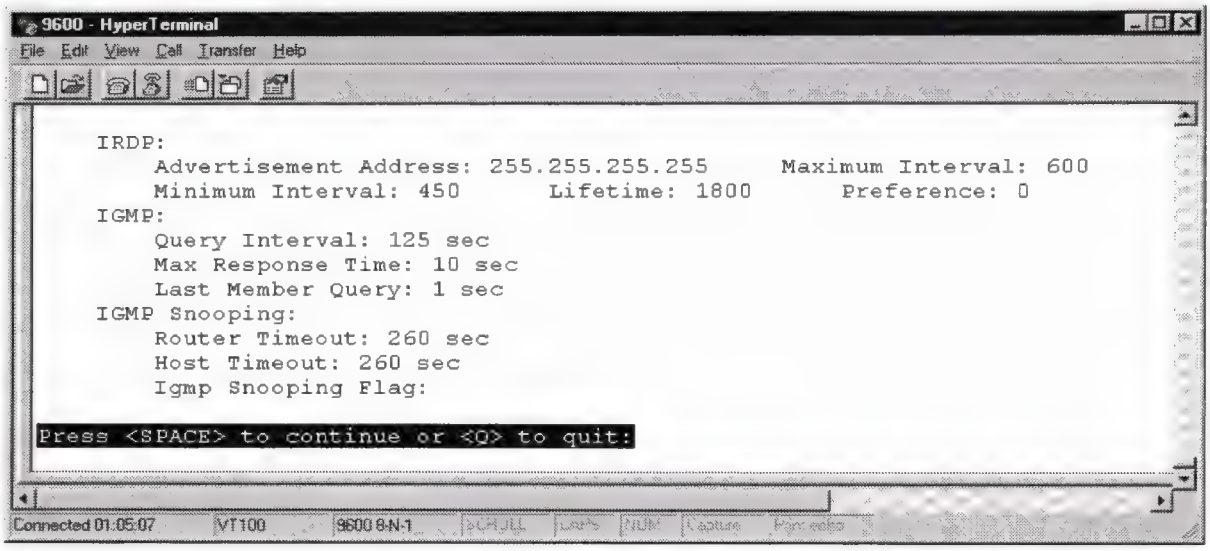
Notes:

Show ipconfig - Global Timers

This portion of the “show ipconfig” display is the global timers information section.

© 2001 Extreme Networks,Inc. All rights reserved

Show ipconfig
Global Timers



Notes:

Show ipconfig - VLAN Specific

This is the last portion of the "show ipconfig" display. It contains the VLAN specific information.

Additional verification commands
Additional commands are available for verification of configuration

CLI Command – Show iproute
Show iproute
Displays the currently configured routes, and includes how each route was learned.
CLI Command – Show iparp
show iparp {permanent | proxy {<ipaddress>}| vlan <vlan name> | <ipaddress>}
Displays the IP Address Resolution Protocol (ARP) table. The display can be filtered by IP address, VLAN, or permanent entries.

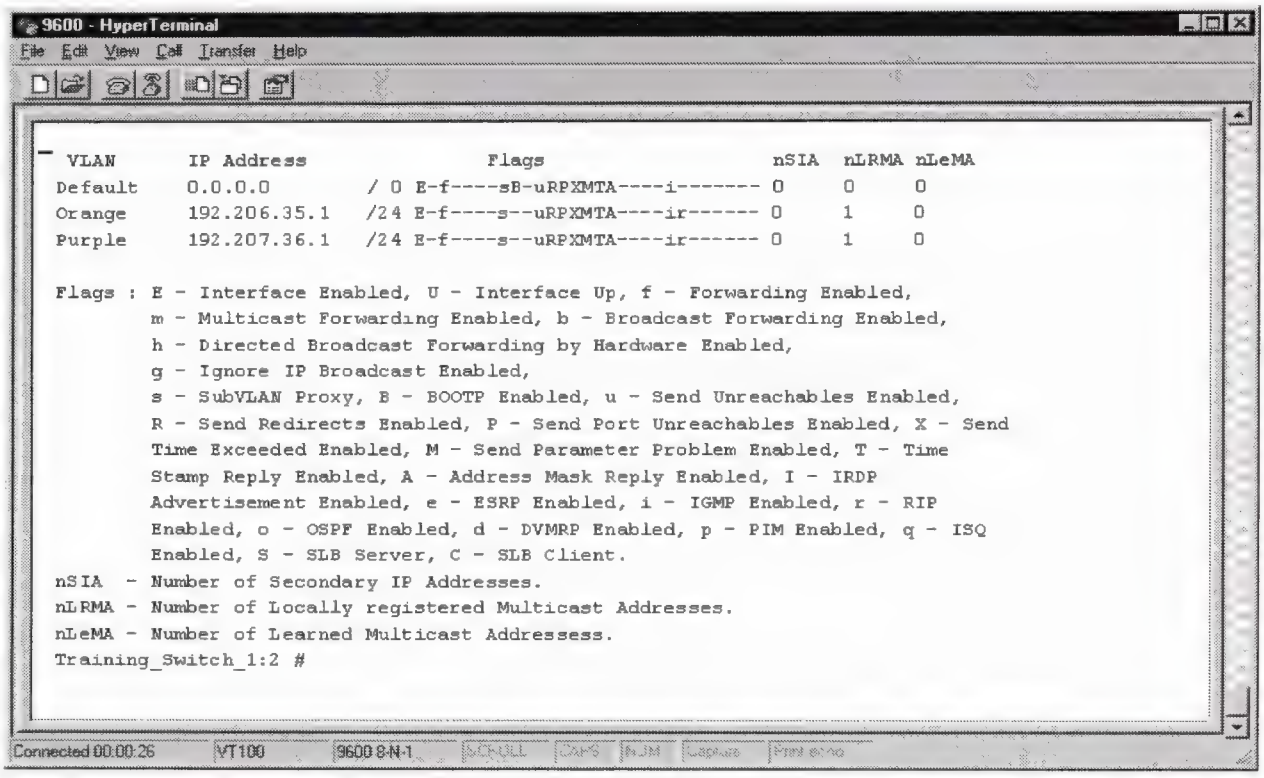
CLI Command – Show ipfdb
show ipfdb {vlan <vlan name> | <ipaddress> / {<netmask>}}
Displays the hosts that have been transmitting or receiving packets, and the port and VLAN for each host.

CLI Command – Show ipconfig
show ipconfig
Displays configuration information for one or more VLANs.

CLI Command – Show ipstats
Show ipstats {vlan <vlan name> | <ipaddress>}
Displays IP statistics for the CPU of the switch.

© 2001 Extreme Networks,Inc. All rights reserved

Show ipconfig
VLAN Specific


9600 - HyperTerminal
File Edit View Call Transfer Help
VLAN IP Address Flags nSIA nLRMA nLeMA
Default 0.0.0.0 / 0 E-f----sB-uRPXMTA----i------- 0 0 0
Orange 192.206.35.1 /24 E-f----s--uRPXMTA----ir------ 0 1 0
Purple 192.207.36.1 /24 E-f----s--uRPXMTA----ir------ 0 1 0
Flags : E - Interface Enabled, U - Interface Up, f - Forwarding Enabled,
m - Multicast Forwarding Enabled, b - Broadcast Forwarding Enabled,
h - Directed Broadcast Forwarding by Hardware Enabled,
g - Ignore IP Broadcast Enabled,
s - SubVLAN Proxy, B - BOOTP Enabled, u - Send Unreachables Enabled,
R - Send Redirects Enabled, P - Send Port Unreachables Enabled, X - Send
Time Exceeded Enabled, M - Send Parameter Problem Enabled, T - Time
Stamp Reply Enabled, A - Address Mask Reply Enabled, I - IRDP
Advertisement Enabled, e - ESRP Enabled, i - IGMP Enabled, r - RIP
Enabled, o - OSPF Enabled, d - DVMRP Enabled, p - PIM Enabled, q - ISQ
Enabled, S - SLB Server, C - SLB Client.
nSIA - Number of Secondary IP Addresses.
nLRMA - Number of Locally registered Multicast Addresses.
nLeMA - Number of Learned Multicast Addressess.
Training_Switch_1:2 #
Connected 00:00:26 VT100 9600 8-N-1

Notes:

Summary

The main theme of chapter eight has been to discuss the Layer 3 unicast routing fundamentals, primarily IP forwarding, IP routing functionality and configuration available on the Extreme Networks range of switches. You should now be able to:

- Describe Layer 3 Operations and differentiate between IP forwarding and Routing Function
- Discuss ExtremeWare supported IP features
- Define RIF, IP Route Tables and IPFDB
- Describe how to populate entries in the IPFDB and IP Route Table
- Configure IP Unicast Routing
- Successfully complete lab exercises

© 2001 Extreme Networks,Inc. All rights reserved

Summary

You should now be able to:

- **Describe Layer 3 Operations and differentiate between IP forwarding and Routing Function**
- **Discuss ExtremeWare supported IP features**
- **Define RIF, IP Route Tables and IPFDB**
- **Describe how to populate entries in the IPFDB and IP Route Table**
- **Configure IP Unicast Routing**
- **Successfully complete lab exercises**

Notes:

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 9

RIP Configuration

Chapter Objectives

The main theme of chapter nine is to discuss the IP Unicast routing protocols RIP v1 and RIP v2, available on the Extreme Networks range of switches.

Upon completion of this chapter, you will be able to:

- Provide a brief overview of RIP
- Describe the routing table using RIP
- Describe the RIP Route Advertisement of VLANs
- Discuss RIP Configuration Example
- Utilise RIP CLI Configuration Commands
- Successfully complete the RIP Lab exercise (Optional)

It is assumed that students are already familiar with IP Unicast routing. If not, it is recommended that you refer to the following publications for additional information:

- RFC 1058 – Routing Information Protocol (RIP)
- RFC 1256 – ICMP Router Discovery Messages
- RFC 1723 – RIP Version 2
- Book: Interconnections: Bridges and Routers by Radia Perlman
  ISBN 0-201-56332-0. Published by Addison-Wesley Publishing Company

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

Upon completion of this chapter, you will be able to:

- **Provide a brief overview of RIP**
- **Describe the routing table using RIP**
- **Describe the RIP Route Advertisement of VLANs**
- **Discuss RIP Configuration Example**
- **Utilise RIP CLI Configuration Commands**
- **Successfully complete the RIP Lab exercise (Optional)**

Notes:

Manual Configuration?

As the network grows in size and complexity, the problem of manually determining the best route for information to follow becomes a bigger problem. Some of the issues faced include:

- How to populate a large number of routing tables
- How to cope with a changing topology
- How to provide resiliency
- How to allow for future growth of the network

To resolve these issues we need to implement a mechanism to populate the route tables and resolve the other issues in an automated fashion.

The solution to these problems is to implement a routing function within the network design.

The Extreme Networks range of switches incorporates this functionality as a separate routing function. The routing function in the switch is defined by the particular routing protocol it supports.

Supported protocols include:

- RIP1 - Routing Information Protocol Version 1
- RIP2 - Routing Information Protocol Version 2
- OSPF - Open Shortest Path First
- BGP – Border Gateway Protocol v4

© 2001 Extreme Networks,Inc. All rights reserved

Manual Configuration ?

- **What if you have 50 switches and 500 devices, what now?**

Notes:

Utilise RIP - A Routing Protocol

RIP is an Interior Gateway Protocol (IGP). Its early predecessor was first used in computer routing in the Advanced Research Projects Agency Network (ARPAnet) as early as 1969. It is primarily intended for use in homogeneous networks of moderate size.

To determine the best path for a distant network, a router using RIP always selects the path that has the least number of hops. Each router that data must traverse is considered to be one hop.

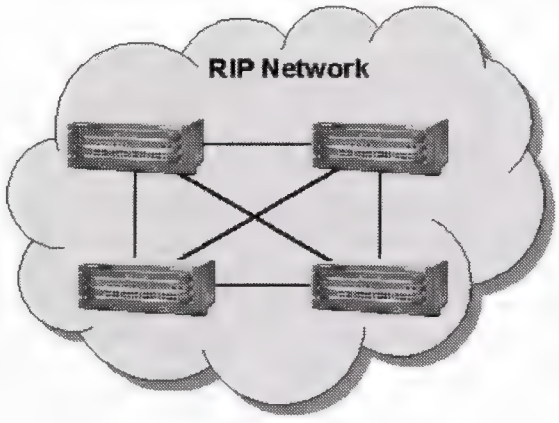
Using a distance-vector protocol, each router creates a unique routing table from summarised information obtained from neighbouring routers. This is based on the Bellman-Ford (distance-vector) algorithm. The distance-vector algorithm has been in use for many years, and is widely deployed and understood.
The biggest advantage of using RIP is that it is relatively simple to understand and implement, and it has been a *de facto* routing standard for many years.

The distinction between RIP and other routing protocols like OSPF lies in the fundamental differences between distance-vector protocols and link-state protocols. These are discussed later in the course.

© 2001 Extreme Networks,Inc. All rights reserved

Utilise RIP – A Routing Protocol

- A distance-vector protocol used as an IGP
- Relatively simple to understand and implement,
- Each router creates its routing table based on route information exchanged between neighbours.
- Supported by all Extreme switches



Notes:

More on RIP

RIP depends upon each router notifying its neighbours when there is a change in its routing table. However, if a router crashes, it cannot notify its neighbours of a change. In order to handle these types of problems, distance-vector protocols must have the ability to remove old routes (not updated) from the routing table based on a timeout procedure.

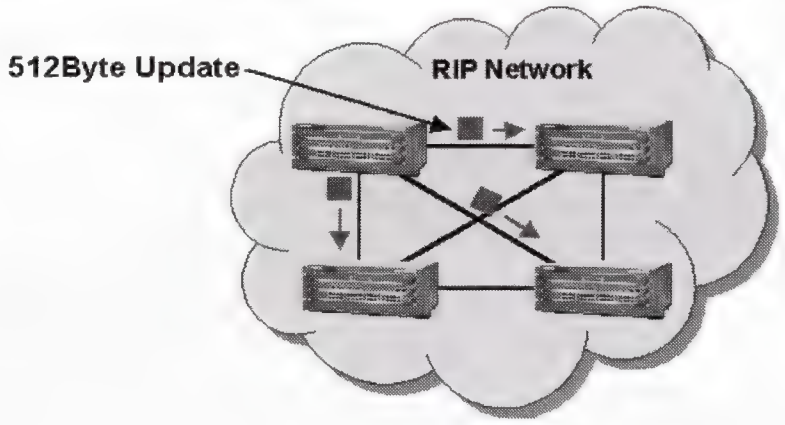
All routers participating in RIP send update messages at every update interval. The default value is *30 seconds*. If a router does not receive an update message within six update cycles (nominally 180 seconds) from the router that was the source of the original routing table entry, it assumes that either the source router has failed or that the connecting link has become unusable. The router marks the existing route as invalid and eventually removes the route from its routing table. When the router learns of a new route from another neighbour, the new route is used to replace the deleted one.
Periodically, each RIP router will send a routing table update message to every neighbour. This update message will contain the information from the device's routing table, as it currently exists. If the information contained in the routing table is too large to fit into a single RIP update message, it will be divided and placed into as many messages as needed to convey the entire routing table. Each message can contain 25 route advertisements and be a maximum of 512 bytes long.

Triggered Updates are a way to bypass the 30-second interval between RIP updates. Essentially they allow a router to inform its neighbours of a change to its routing table immediately that change occurs, without having to wait for the next 30-second update interval. These are covered in greater detail later in this chapter.

© 2001 Extreme Networks,Inc. All rights reserved

More on RIP

- The router exchanges update messages with each neighbour every 30 seconds.
- In RIP V1, 25 routes can be advertised in a single packet. This limits the maximum packet size to 512 octets
- Support 2 types of loop resolution protocols
- Reporting static routes
- Triggered updates – don't have to wait 30 seconds if something happened.



Notes:

Resolution Protocols Supported in RIP

A number of modifications can be made to the basic distance-vector routing algorithm to improve performance in a dynamic environment and to help expedite convergence and eliminate routing loops. These include:

- Split-horizon
- Poison reverse

By default, both are enabled on Extreme Networks switches.

The slide shows how a loop is created between two routers:

- Router B reaches the target network with a hop count of one using Router A
- Router C learns in its regular update from Router B that it reaches the target network using Router B with a hop count of two

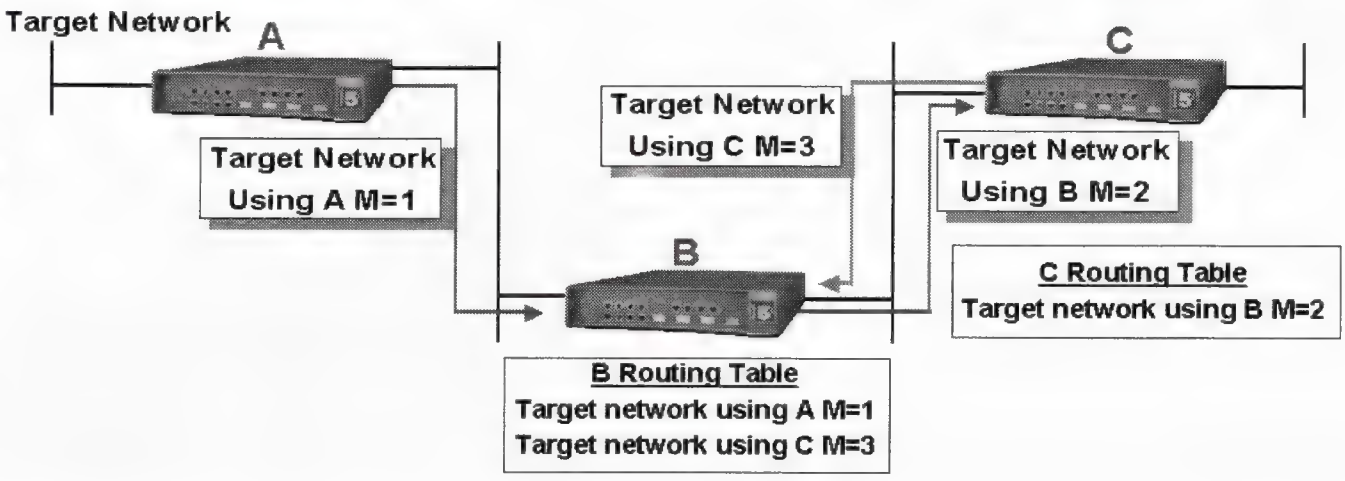
In Router C's next update, it advertises reachability to the target network back to Router B with a hop count of three. As a result, Router B now has two routes to the target network; the first using Router A with a hop count of one, the second using Router C with a hop count of three. Router B chooses the route using Router A, since Router A has the smallest total hop count.

If the link between Router A and Router B fails, Router B does not receive an update from Router A in the required time and will timeout the route to the target network through Router A. Remember that Router B has a secondary route to the target network using Router C with a hop count of three. Router B now forwards all traffic destined for the target network to Router C. Router C, in turn, forwards the traffic back to Router B. As a result of this mutual deception, a loop of size two is created. A packet will travel back and forth between Router B and Router C until the time to live field in the IP header is reduced to zero, and the packet is eventually discarded by one of the routers.

© 2001 Extreme Networks,Inc. All rights reserved

Resolution Protocols Supported in RIP

- Used to prevent routing loop
- Two types
  - Split Horizon
  - Poison Reverse
- Both are ENABLED by default on the switch
- Poison Reverse takes precedence over split horizon when both are enabled to prevent loops.



Notes:

Split Horizon

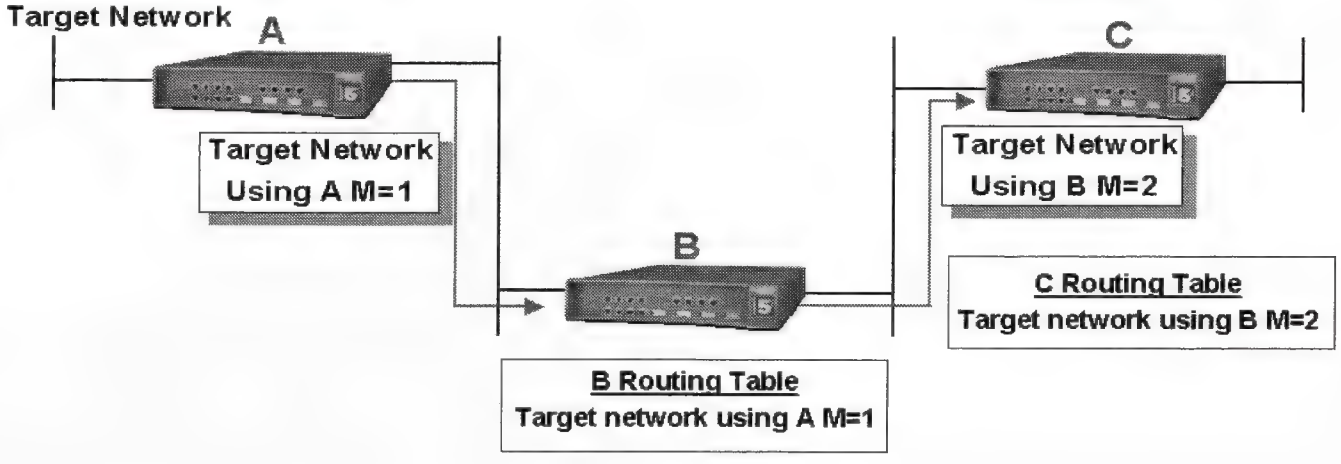
The occurrence of loops between two routers can be greatly reduced by using split-horizon. The count-to-infinity problem can be overcome if the router is careful about where it sends its routing information. Split-horizon is a technique whereby a router does not advertise a route over the same port that supplied the route. In other words, a router does not claim network reachability to a neighbour from which the route was learned.

The slide demonstrates the use of split-horizon to break a loop of two hops. The update procedure is roughly the same, except that Router C does not advertise the route to the target network back to Router B. As a result of split-horizon, Router B has only one route to the target network. If the link between Router A and Router B fails, Router B will timeout the entry and advertise the target network as unreachable. The possibility of a loop has been eliminated.

© 2001 Extreme Networks,Inc. All rights reserved

Split Horizon

- **Router does not propagate a route over the port that supplied the route**
- **The possibility of a loop has been eliminated using split horizon**



Notes:

Poison Reverse

Split-horizon with *poison reverse* is a technique whereby a router advertises a route over the same port that supplied the route with a hop count of 16. A router claims that a network is unreachable over the interface from which the route was learned, preventing any packets destined for the poisoned network from going down hill, away from the most efficient route. Poison reverse speeds up convergence because erroneous routes will not need to be eliminated by waiting for a timeout.

The slide opposite illustrates a typical exchange of routing information when a router is configured to perform split-horizon with poison reverse.

In this example:

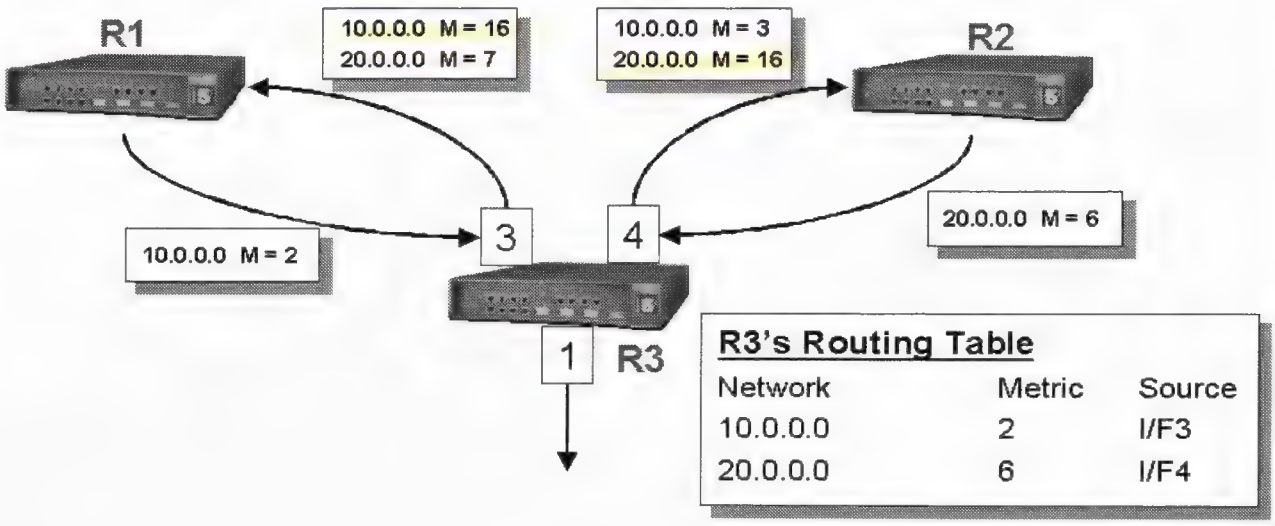
- Router 3 receives an advertisement for Network 10.0.0.0 on Port 3 and an advertisement for Network 20.0.0.0 on Port 4
- Router 3 selects each of these routes, installs them in its routing table, and advertises the routes on Port 1 with adjusted metrics
- Since poison reverse is enabled on Port 3 and the route for Network 10.0.0.0 was learned over Port 3, Router 3 advertises Network 10.0.0.0 on Port 3 with a metric of 16 hops
- The route for Network 20.0.0.0 is adjusted and advertised on Port 3 with a metric of 7. Likewise, Router 3 advertises Network 20.0.0.0 on Port 4 with a metric of 16
- The route for Network 10.0.0.0 is adjusted and advertised on Port 4 with a metric of three

The disadvantage of poison reverse is that it increases the size of the routing update messages. In many cases, the network administrator may be willing to accept slower convergence to reduce the overhead that the increased size of the routing table update messages would cause.

© 2001 Extreme Networks,Inc. All rights reserved

Poison Reverse

- Routers advertise routes with Hop count of 16
- Faster convergence
- Possible increased size of routing messages



Notes:

Triggered Updates

Triggered updates occur whenever a router changes the metric for a route, and it is required to send an update message immediately, even if it is not yet time for a regular update message to be sent. This will generally result in faster convergence, but will also result in more RIP-related traffic.

Triggered updates can cause excessive loads on networks with limited bandwidth or with many routers on them. A simple solution to this problem is to set a timer to a random number between one and five seconds after a triggered update is sent. If other changes occur that would trigger another update before the timer expires, the router must wait until the timer expires before sending the update. A triggered update may also be suppressed if a regular timed update is due by the time the triggered update would be sent.

The slide shows a network in two states:

- Before the triggered update was issued (struck-out entries)
- After all routers have converged their router tables

In the slide opposite, Router A times out its route to the target network. The timeout forces Router A to issue triggered updates on its ports.

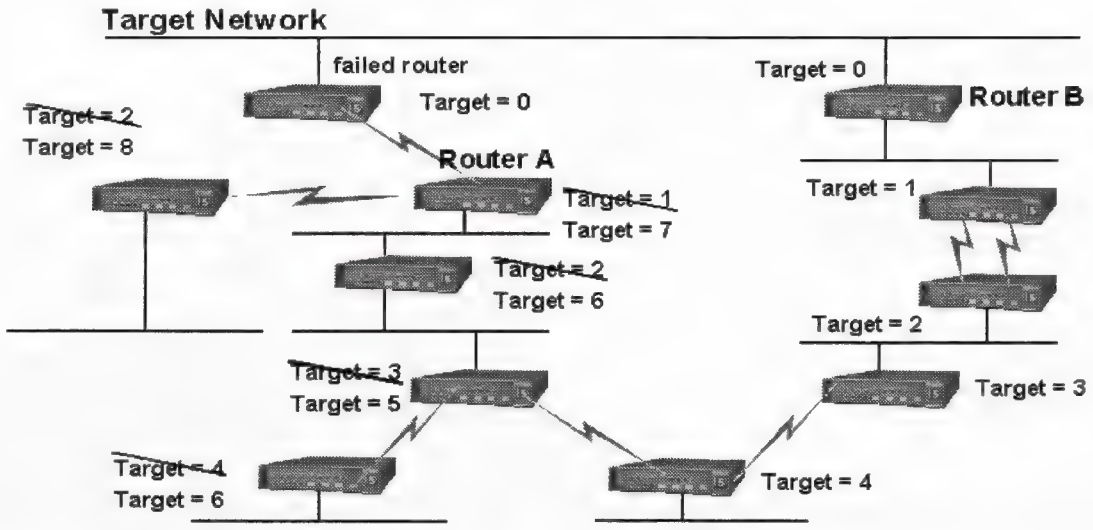
The update propagates backward along all paths that lead to Router A, updating the metric for the target network to infinity (not shown on slide).

The network will converge on the new route to the target network based on the route available through Router B.

© 2001 Extreme Networks,Inc. All rights reserved

Triggered Updates

- **Sent out whenever the metric for a route changes and the router is required to send an update immediately**
  - Even if it is not yet time for a regular update message to be sent.
- **Generally result in faster convergence,**
- **Will result in more RIP-related traffic.**



Notes:

RIP Limitations

Distance-vector routing algorithms have been in use for quite a while, so they are well understood by software developers.

Distance-vector routing algorithms can quickly determine the shortest route to a distant network. However, this can be misleading due to the potential slow convergence problem, which may require multiple updates.

These routes are based on hop count and do not take into account any cost related issues.

Depending on the size and complexity of the network, the amount of information exchanged between neighbours can be quite large.

Each router periodically transmits all its routing information to its neighbours. The information transmitted by each router is based on the information that it receives from its immediate neighbours. Thus, the identification of a router that supplies inaccurate data is quite difficult.

A change in the routing table of a single router can result in a chain of updates. It can take a long time for this information to reach all other routers in the routing domain.

As a result of the slow propagation of routing information, distance-vector routing algorithms can form routing loops and can be slow to converge. This slow convergence can lead to route instability and increased traffic overhead.

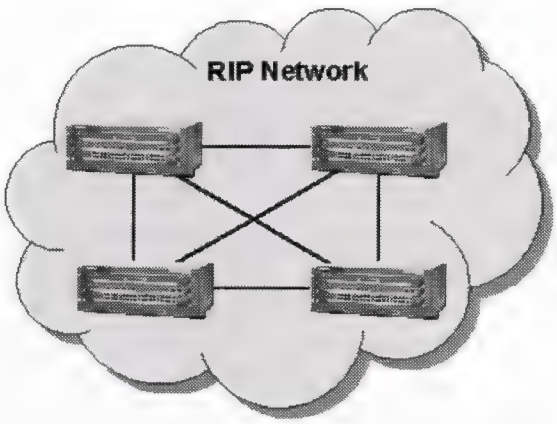
Distance-vector routing algorithms do not scale well and have problems in very large networks because of the potential for slow convergence.

These routing algorithms do not utilise the concept of Areas, rather, the complete network is seen as a single domain.

© 2001 Extreme Networks,Inc. All rights reserved

RIP Limitations

- **Limit of 15 hops between the source and the destination networks**
- **A large amount of bandwidth taken up by periodic broadcasts of entire routing table**
- **Slow convergence** – how long it take everybody to know every route
- **Routing decisions based on hop count;**
  - No concept of link costs or delay
- **Flat networks; no concept of areas or boundaries**



Notes:

RIP Version 1

As previously discussed, RIP is extremely well known and utilised. However, RIP Version 1 does have several limitations. These include:

Classfull Addressing:

- RIP Version 1 only understands class A, B and C addresses

Subnet Masks:

- RIP Version 1 does not propagate subnet mask information

Variable Length Subnet Masks:

- RIP Version 1 does support variable length subnet masks

Generates Broadcasts:

- RIP Version 1 uses broadcasts to deliver routing updates

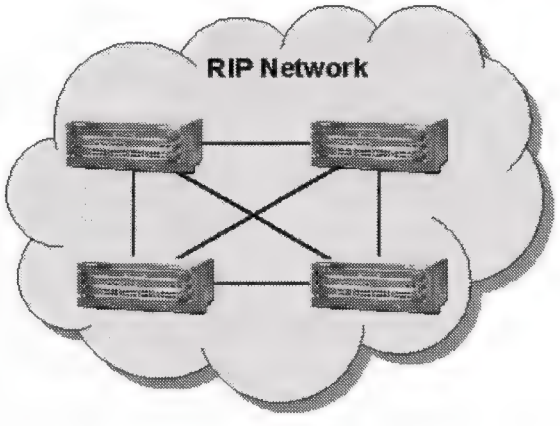
Security:

- RIP Version 1 does not support any authentication and routers sending updates cannot be verified

© 2001 Extreme Networks,Inc. All rights reserved

RIP Version 1

- **Limited because it is a classfull routing protocol**
  - Only understands class A, B, and C addresses
  - Does not propagate subnet mask information in its updates
  - Cannot support variable length subnet masks
- **Uses broadcasts for update delivery**
- **It is an un-secure routing protocol**



Notes:

RIP Version 2

RIP Version 2 (RIPv2) introduces subnet mask information into the Routing Information Protocol to handle variable-length subnetting that has become prevalent in the IP addressing scheme, due to the scarcity of IP addresses. Other benefits of implementing RIPv2 include:

- Variable-Length Subnet Masks (VLSMs)
- Next-hop address
- Support for next-hop addresses allowing for optimisation of routes in certain environments
- Multicasting

RIP Version 2 uses the multicast address **224.0.0.9** for router updates.

RIPv2 packets can be multicast instead of being broadcast, reducing the load on hosts that do not support routing protocols. Using multicasts also allows RIP Version 2 routers to share information, which RIP Version 1 routers cannot receive.

Backward compatibility with existing RIPv1 implementations is an important design criterion. The implementation allows for different compatibility modes to interoperate with both RIPv1 and RIPv2 implementations.

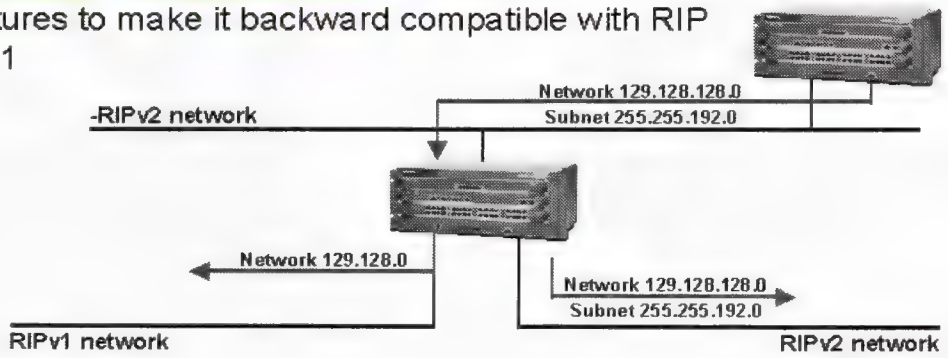
NOTE: If you are using RIP with supernetting/Classless Inter-Domain Routing (CIDR), you must use RIPv2 only. In addition, RIP route aggregation must be turned off.

10.10.0.0
10.20.0.0 , different subnets

© 2001 Extreme Networks,Inc. All rights reserved

RIP Version 2

- **Fixed many of the limitations with RIP-1**
  - Is a classless routing protocol
  - Supports variable length subnet masking
  - Supports CIDR (Classless Internet Domain Routing)
  - Supports Autonomous Domains
  - Supports Authentication (not supported in ExtremeWare V6.1.8)
    - Clear text password
    - MD5 – checksum (RFC 2082)
  - Uses multicast for update delivery (P354)-
  - Has features to make it backward compatible with RIP Version 1



Notes:

Routing Table for Router using RIP

The routing table in each device using RIP, contains an entry for every known destination network. Each routing table entry contains the following information:

- IP address of the destination network
- Metric (hop count) to the destination network
- IP address of the next router
- Timer that tracks the amount of time since the entry was last updated

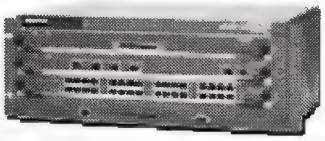
The router exchanges an update message with each neighbour every 30 seconds (default value), or if there is a change to the overall routed topology (also called ***triggered updates)***. If a router does not receive an update message within six update cycles (nominally 180 seconds) from the router that was the source of the original routing table entry, it assumes that either the source router has failed or that the connecting link has become unusable. The router marks the existing route as invalid and eventually removes the route from its routing table. When the router learns of a new route from another neighbour, the new route is used to replace the deleted one.

The distance-vector routing algorithm waits for six times the update interval before timing out the route, even though it expects to hear from each neighbour at every update interval. The additional time is used to avoid invalidating routes based on the loss of a single update message

© 2001 Extreme Networks,Inc. All rights reserved

Routing Table For Router using RIP

- **Contains an entry for every known destination network**
- **Contains the following information**
  - IP Address of destination network
  - Metric (hop count) to the destination network
  - IP address of the next router
  - Timer that tracks the amount of time since last entry update



Route Table

Address	Metric	Gateway	Ticks how long it get my last update
194.101.11.0	5	158.111.1.2	10
168.201.1.3.0	2	158.111.1.2	15

Notes:

RIP Configuration Example

This shows the CLI commands required to configure RIP on the Extreme Networks products to ensure that routes will be advertised for the VLANs configured for RIP.

VLANs that are configured with an IP address, but are configured to not forward IP or are not configured to run RIP, do not have their subnets advertised by RIP. Only those VLANs that are configured with an IP address and are configured to forward IP and run RIP have their subnets advertised.

Further CLI commands associated with RIP:

CLI Command – configure rip add/delete vlan
configure rip add vlan [all | <vlan name>] <cr>
configure rip delete vlan [all | <vlan name>] <cr>

Configures/Disables RIP on an IP interface. You must specify either a VLAN name or all (i.e. all VLANs). When an IP interface is created, per-interface RIP configuration is disabled by default.

When RIP is disabled on the interface, the parameters are not reset to their defaults.
CLI Command – enable/disable rip
enable rip <cr>
disable rip <cr>
Enables/disables RIP globally on the switch. The default setting is disabled.

CLI Command – show rip
show rip [detail | stats | vlan <vlan name>] <cr>
Displays RIP configuration and statistics for one or all VLANs.

CLI Command – show rip statistics
show rip stats [detail | vlan <vlan name>] <cr>
Displays RIP-specific statistics for one or all VLANs
.

© 2001 Extreme Networks,Inc. All rights reserved

RIP Configuration Example

- **Create and configure VLANs**
  - create vlan vlanrip
  - conf vlanrip add ports 1-4
- **Configure VLAN with an IP address**
  - conf vlanrip ipaddress 10.10.10.1/24
- **Enable IP Forwarding**
  - enable ipf
- **Enable RIP on VLANs that will do routing**
  - conf rip add vlan vlanrip
- **Enable RIP globally on the switch**
  - enable rip
- **Verify RIP configuration- "show rip" & "show ipconf"**

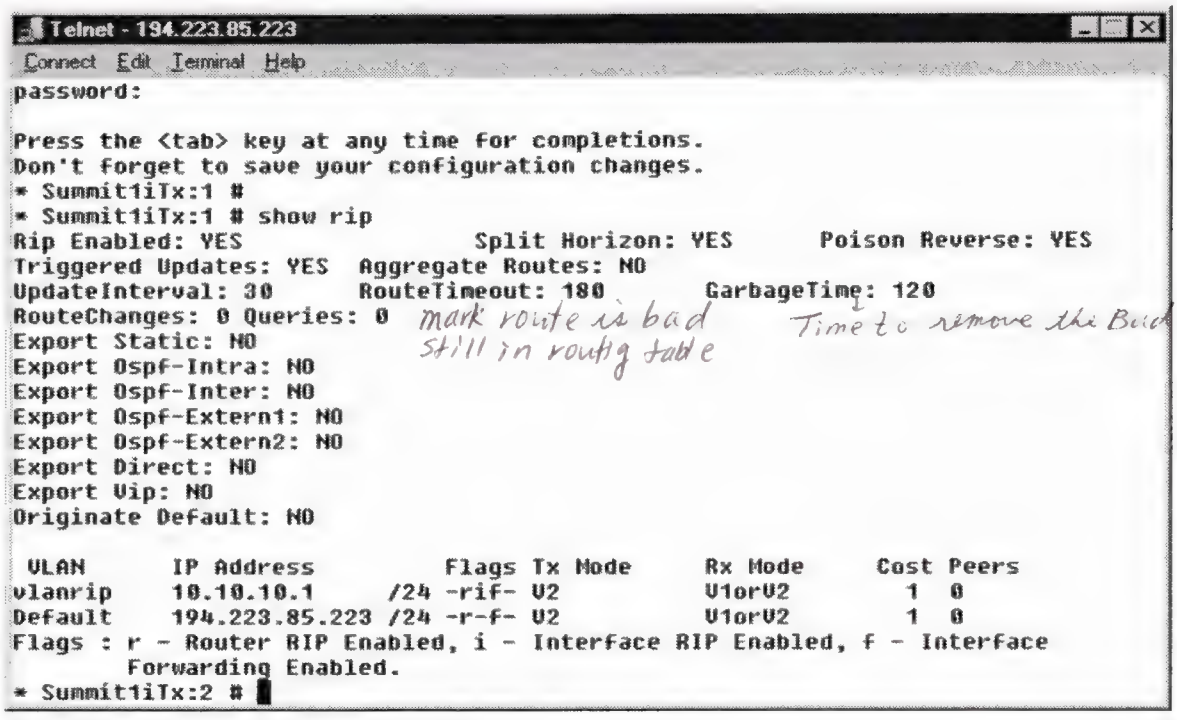
Notes:

Example - show rip

This Telnet session shows the information supplied by the switch in response to a "show rip" CLI command.

© 2001 Extreme Networks,Inc. All rights reserved

Example - show rip


Telnet - 194.223.85.223
Connect Edit Terminal Help
password:
Press the <tab> key at any time for completions.
Don't forget to save your configuration changes.
* Summit1iTx:1 #
* Summit1iTx:1 # show rip
Rip Enabled: YES Split Horizon: YES Poison Reverse: YES
Triggered Updates: YES Aggregate Routes: NO
UpdateInterval: 30 RouteTimeout: 180 GarbageTime: 120
RouteChanges: 0 Queries: 0
Export Static: NO
Export Ospf-Intra: NO
Export Ospf-Inter: NO
Export Ospf-Extern1: NO
Export Ospf-Extern2: NO
Export Direct: NO
Export Vip: NO
Originate Default: NO
VLAN IP Address Flags Tx Mode Rx Mode Cost Peers
vlanrip 10.10.10.1 /24 -rif- U2 U1orU2 1 0
Default 194.223.85.223 /24 -r-f- U2 U1orU2 1 0
Flags : r - Router RIP Enabled, i - Interface RIP Enabled, f - Interface
Forwarding Enabled.
* Summit1iTx:2 #
mark route is bad
still in routing table
Time to remove the Bad Route

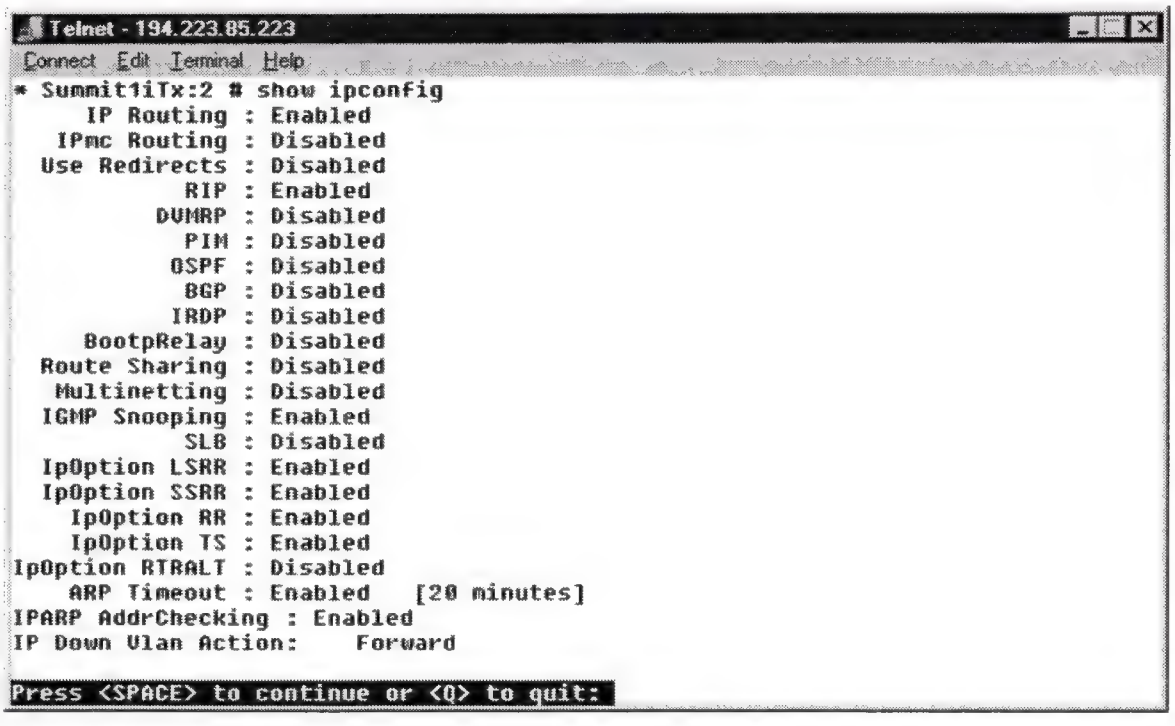
Notes:

Example - show ipconfig

This Telnet session shows the information supplied by the switch in response to a "show ipconfig" CLI command.

© 2001 Extreme Networks,Inc. All rights reserved

Example – "show ipconfig"



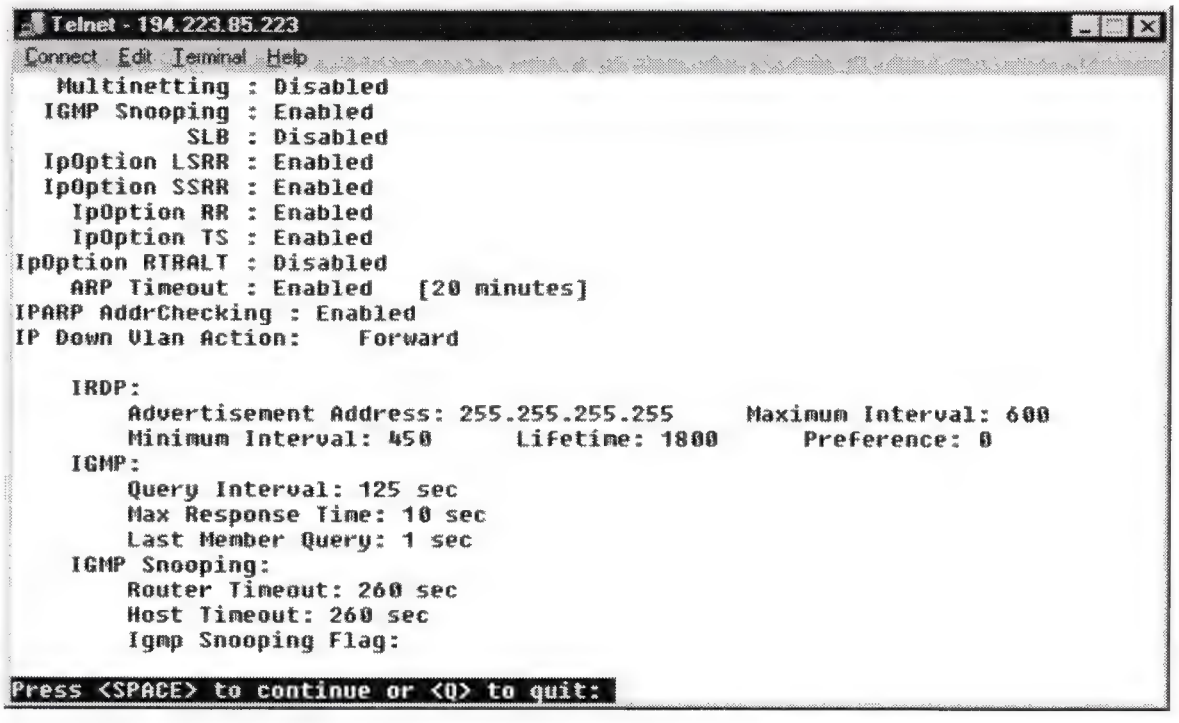
Notes:

Example - show ipconfig continued...

This Telnet session shows the information supplied by the switch in response to a "show ipconfig" CLI command.

© 2001 Extreme Networks,Inc. All rights reserved

Example – "show ipconfig" cont…


Telnet - 194.223.85.223
Connect Edit Terminal Help
Multinetting : Disabled
IGMP Snooping : Enabled
SLB : Disabled
IpOption LSRR : Enabled
IpOption SSRR : Enabled
IpOption RR : Enabled
IpOption TS : Enabled
IpOption RTRALT : Disabled
ARP Timeout : Enabled [20 minutes]
IPARP AddrChecking : Enabled
IP Down Vlan Action: Forward
IRDP:
Advertisement Address: 255.255.255.255 Maximum Interval: 600
Minimum Interval: 450 Lifetime: 1800 Preference: 0
IGMP:
Query Interval: 125 sec
Max Response Time: 10 sec
Last Member Query: 1 sec
IGMP Snooping:
Router Timeout: 260 sec
Host Timeout: 260 sec
Igmp Snooping Flag:
Press <SPACE> to continue or <Q> to quit:

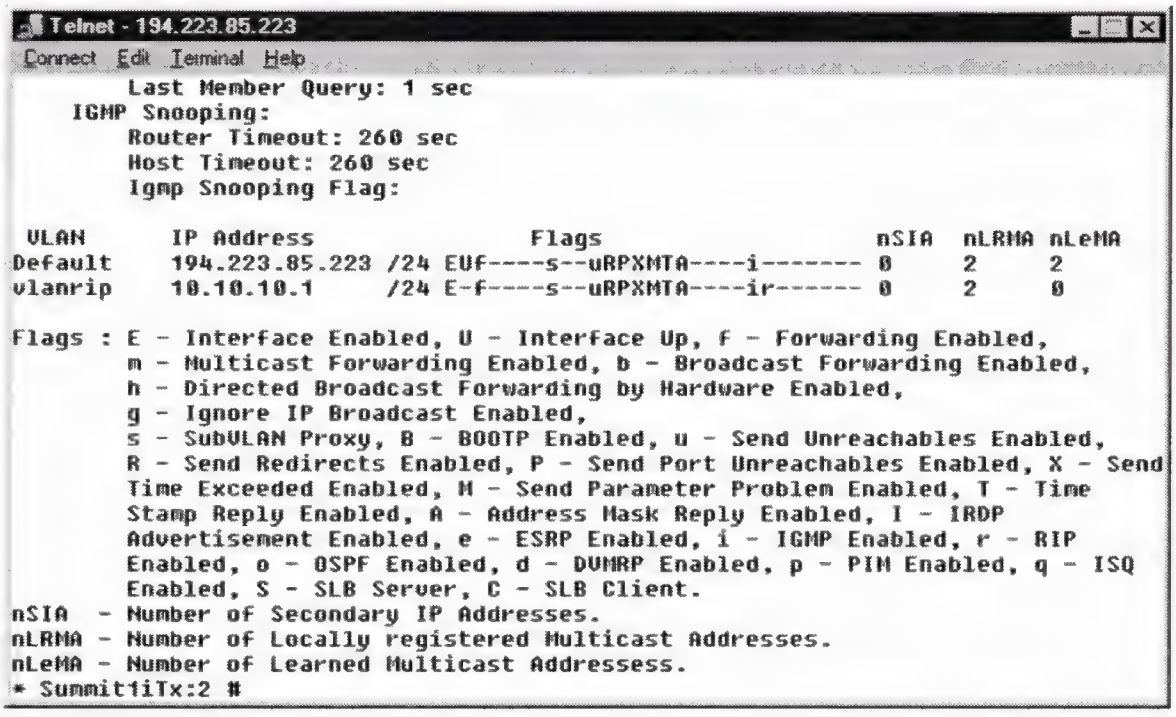
Notes:

Example - show ipconfig continued

This Telnet session shows the information supplied by the switch in response to a “show ipconfig” CLI command.

© 2001 Extreme Networks,Inc. All rights reserved

Example – "show ipconfig" cont...


Telnet - 194.223.85.223
Connect Edit Terminal Help
Last Member Query: 1 sec
IGMP Snooping:
Router Timeout: 260 sec
Host Timeout: 260 sec
Igmp Snooping Flag:
VLAN IP Address Flags nSIA nLRMA nLeMA
Default 194.223.85.223 /24 EUf----s--uRPXMTA----i------- 0 2 2
vlanrip 10.10.10.1 /24 E-f----s--uRPXMTA----ir------ 0 2 0
Flags : E - Interface Enabled, U - Interface Up, f - Forwarding Enabled,
m - Multicast Forwarding Enabled, b - Broadcast Forwarding Enabled,
h - Directed Broadcast Forwarding by Hardware Enabled,
g - Ignore IP Broadcast Enabled,
s - SubVLAN Proxy, B - BOOTP Enabled, u - Send Unreachables Enabled,
R - Send Redirects Enabled, P - Send Port Unreachables Enabled, X - Send
Time Exceeded Enabled, M - Send Parameter Problem Enabled, T - Time
Stamp Reply Enabled, A - Address Mask Reply Enabled, I - IRDP
Advertisement Enabled, e - ESRP Enabled, i - IGMP Enabled, r - RIP
Enabled, o - OSPF Enabled, d - DVMRP Enabled, p - PIM Enabled, q - ISQ
Enabled, S - SLB Server, C - SLB Client.
nSIA - Number of Secondary IP Addresses.
nLRMA - Number of Locally registered Multicast Addresses.
nLeMA - Number of Learned Multicast Addressess.
* Summit1iTx:2 #

Notes:

Summary

The main theme of chapter nine has been to discuss the IP Unicast routing protocols RIP v1 and RIP v2, available on the Extreme Networks range of switches. You should now be able to:

- Provide a brief overview of RIP
- Describe the routing table using RIP
- Describe the RIP Route Advertisement of VLANs
- Discuss RIP Configuration Example
- Describe RIP CLI Configuration Commands
- Successfully complete the RIP Lab exercise (Optional)

© 2001 Extreme Networks,Inc. All rights reserved

Summary

You should now be able to:

- **Provide a brief overview of RIP**
- **Describe the routing table using RIP**
- **Describe the RIP Route Advertisement of VLANs**
- **Discuss RIP Configuration Example**
- **Describe RIP CLI Configuration Commands**
- **Successfully complete the RIP Lab exercise (Optional)**

Notes:

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 10

OSPF Overview and Configuration

Chapter Objectives

The main theme of chapter ten is to discuss the IP routing protocol Open Shortest Path First (OSPF), available on the Extreme Networks range of switches. Upon completion of this chapter, you will be able to:

- Define OSPF as a routing protocol
- Describe how to build OSPF Networks
- Define OSPF Areas, router types and virtual links
- Describe how OSPF operates
- Define LSA, LSDB, initial synchronisation, database exchange and reliable flooding
- Describe OSPF Configuration and examples
- Successfully complete the lab exercises

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

Upon completion of this chapter, you will be able to:

- **Define OSPF as a routing protocol**
- **Describe how to build OSPF Networks**
- **Define OSPF Areas, router types and virtual Links**
- **Describe how OSPF Operates**
- **Define LSA, LSDB, Initial synchronisation, database exchange & reliable flooding**
- **Describe OSPF Configuration and Examples**
- **Successfully complete the lab exercises**

Notes:

OSPF Defined

The Open Shortest Path First protocol, OSPF, is an IP routing protocol that is classified as an interior gateway protocol (IGP), and offers several advantages over the use of RIP:

Faster convergence

- OSPF quickly responds to topology changes and calculates new loop free routes

Less use of network resources

- OSPF generates less network traffic than RIP as individual packets are smaller and multicasting technology is utilised

Offers greater features

- OSPF calculates the best route based on at least a cost factor, not a hop count
- OSPF offers greater scalability than RIP as it is not limited to a maximum hop count
- OSPF allows for load sharing over routes
- All OSFP routing exchanges can be authenticated

OSPF employs a link-state routing algorithm. The important features of a link-state routing protocol over a distance-vector protocol (like RIP) are:

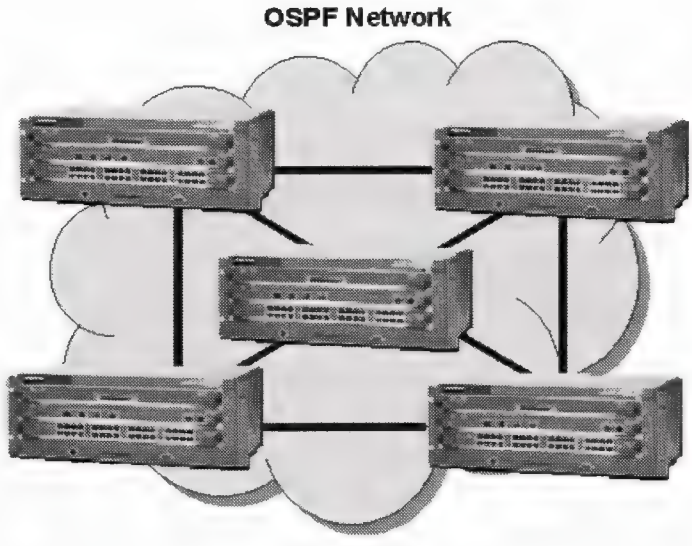
- All routers within a routing domain share information about their interfaces, or links, to directly connected networks
- The link information is stored in a database. This topological database contains a complete description of which routers are connected to which networks in the given domain
- Following convergence, each router has an identical copy of the link-state database from its own perspective

Each router uses the common link-state database (LSDB) to calculate a shortest-path tree to all destinations. The shortest-path tree is then used to create the routing table. Where several equal cost routes exist to a destination, traffic can be distributed among them.

© 2001 Extreme Networks,Inc. All rights reserved

OSPF Defined

- **Dynamic Routing Protocol**
  - It is an interior gateway protocol (IGP)
  - More efficient than RIP
  - Consumes fewer network resources
  - Highly scaleable
  - Faster convergence
  - A more descriptive routing metric
  - Route load sharing
  - Greater security
- **Link State Type of Protocol**
  - Employs a distributed database model



Notes:

OSPF as a Link-State Protocol

OSPF employs a link-state routing algorithm. Each router initially transmits a description of its interfaces (links) to its neighbours. The description that each router sends to its neighbours is called a Router Link State Advertisement (LSA) message. The Router LSA contains a description for each link that includes:

- The IP network number assigned to the link
- The subnet mask assigned to the link
- The metric associated with the link
- The operational status of the link (up or down)

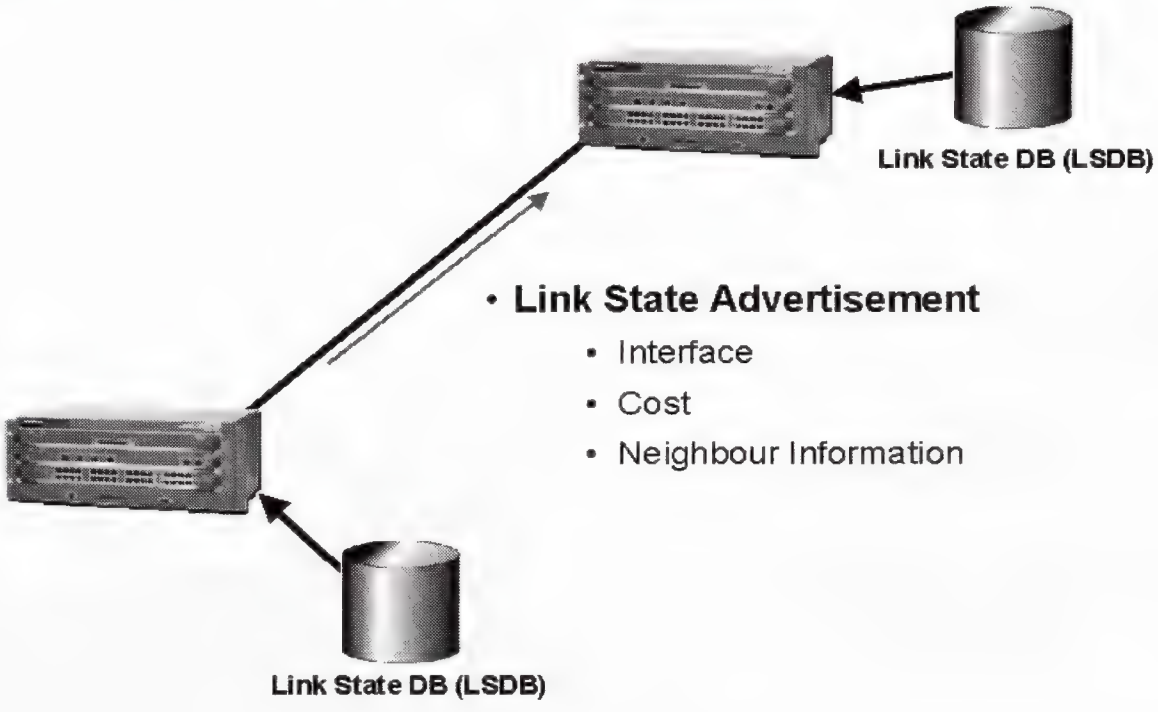
The link information is stored in a database (LSDB) that is synchronised between routers. This database is used to derive the lowest cost route to the destination network.

OSPF maintains one database per area (discussed later), this means that when a router has interfaces in multiple areas, the router must have multiple LSDBs.

Once all routers in an area agree on the state of the LSDB, they periodically exchange very short "Hello" messages which can effectively be thought of as "Hello, I am still here and nothing has changed". Each router in an area expects to receive Hello messages from it's neighbours periodically and if it fails to do so, it assumes that a neighbour (and it's links) is "dead". If a router detects a link state change at any time, it immediately transmits a revised LSA to it's neighbours.

© 2001 Extreme Networks,Inc. All rights reserved

OSPF as a Link-State Protocol



- **Link State Advertisement**
  - Interface
  - Cost
  - Neighbour Information

Notes:

Building OSPF Networks

The next section focuses on building OSPF networks and introduces several concepts and building blocks associated with this task. These include:

- The various OSPF Network types
- The OSPF Routing hierarchy
- How OSPF Areas operate and the different types
- The different types of OSPF routers and interfaces
- The concept and use of Virtual Links

© 2001 Extreme Networks,Inc. All rights reserved

Building OSPF Networks

- OSPF Network Types
- OSPF Routing Hierarchy
- OSPF Areas
- OSPF Types of Routers
- Concept of Virtual Links

Notes:

OSPF Network Types

OSPF is used by a number of wide area network vendors, as it offers three important features:

- Standardization and vendor interoperability
- Scalability
- Low inter-nodal update traffic

Part of the process that OSPF uses to achieve this is to classify networks according to their characteristics, and associate procedures of OSPF according to these classifications (covered later).

Some of the network types defined (those that are associated with WAN technology) are not supported by Extreme Networks, and are defined as:

- Non-broadcast Multi-access (NBMA) networks, for example X.25, ATM and Frame Relay (which is NBMA by default)
- Point-to-Multipoint (PMP) networks, for example, Frame Relay (if it is configured to support PMP)

Network types that are supported by Extreme Networks are:

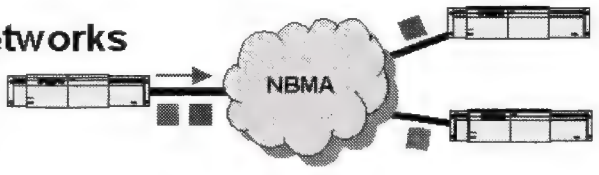
- Point-to-Point networks, for example, leased lines and ADSL
- Broadcast networks, for example, Ethernet

Broadcast networks provide support for multiple attached routes together with the ability to address a single physical message to all the attached devices (e.g. a layer 2 broadcast message).

© 2001 Extreme Networks,Inc. All rights reserved

OSPF Network Types

- **Non-broadcast Multi-access (NBMA) networks**
  - X.25, ATM
  - Not supported by Extreme Networks



- **Point-to-Multipoint networks**
  - Frame Relay
  - Not supported by Extreme Networks

- **Point-to-Point networks**
  - Serial lines, ADSL
  - This Network type is supported by ExtremeWare

- **Broadcast networks (e.g. Ethernet)**
  - This Network type is supported by ExtremeWare

Notes:

OSPF Routing Hierarchy

Implementing a hierarchy in the routing topology of a network dramatically enhances its support for larger network designs.

OSPF implements a two level hierarchical routing scheme that consists of an overall Autonomous System (AS) that contains one or more areas.

An Area consists of one or more physical networks (e.g. several VLANs and/or LANs) connected together via IP routers.

By creating a hierarchy within the OSPF LSDB, larger inter-networks benefit as it:

- Saves router memory consumed by the LSDB and routing table, as each router's LSDB only contains the LSAs for the area it is a member of
- Saves router resources when computing the routing table. The LSDB contains fewer entries, resulting in the OSPF algorithm consuming less CPU time to complete
- Saves link bandwidth when distributing routing data because any topological change is only sent within the effected area

Overall OSPF saves network resources and bandwidth because not every link-state change is propagated to all routers in the AS. This limits the number of routers having to perform a recalculation of the OSPF routing table.

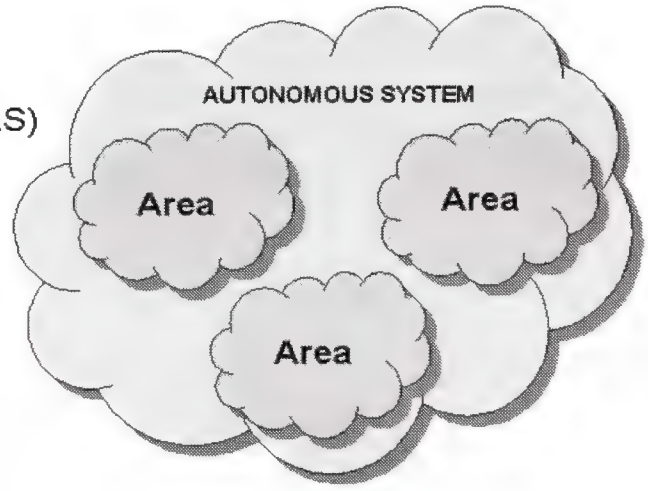
The AS may contain several areas, all of which share a common administration and common design strategy. The term 'Domain' is often used in replace of AS.

© 2001 Extreme Networks,Inc. All rights reserved

OSPF Routing Hierarchy

- **Two-levels of Hierarchy**
  - Between Autonomous Systems (AS)
  - Areas within an AS

50 areas/with 50 routers
→ 50·50 = >500



- **Allows you to save on**
  - Router memory consumed by the LSDB and routing table
  - Router resources when computing the routing table
  - Link bandwidth when distributing routing data
  - Router resources and link bandwidth due to topology changes

Notes:

What is an Autonomous System (AS)?

The classic definition of an **Autonomous System** is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS, and using an exterior gateway protocol to route packets to other ASs.

To the outside world, the whole AS is viewed as one single entity. Each AS has an identifying number, which is assigned to it by an Internet Registry or provider. Routing information between ASs is exchanged via an exterior gateway protocol such as BGP4.

Since this classic definition was developed, it has become common for a single AS to use several interior gateway protocols and sometimes several sets of metrics within an AS.

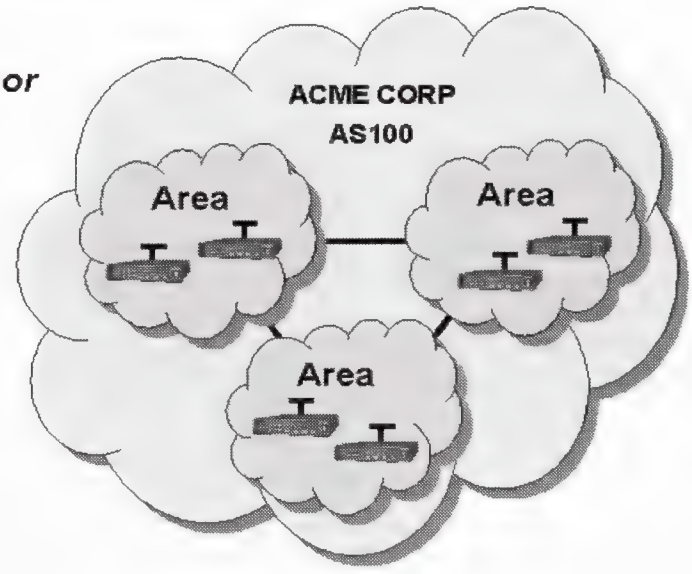
*The use of the term **Autonomous System** here stresses the fact that, even when multiple IGPs and metrics are used, the administration of an AS appears to other ASs to have a single coherent interior routing plan and presents a consistent picture of what destinations are reachable through it.*

© 2001 Extreme Networks,Inc. All rights reserved

What is an Autonomous System (AS)?

- A collection of routers & networks
- Controlled by a single administration
- Bounded by Autonomous System Boundary Routers, ASBR

The AS number is not required or used by OSPF



Notes:

OSPF Areas

OSPF allows the grouping of contiguous networks (LANs, WANs, Point-to-Point links, etc) and hosts into an *Area*. The flooding of Router LSAs is restricted to the area in which they originate such that routers that have interfaces within an area contain a LSDB that contains the "details" of that area. The Shortest Path First (SPF) is computed on a per-area basis, and all intra-area routes are derived from the SPF tree.

The interfaces of each OSPF router are assigned an AreaID. The AreaID is expressed in dotted decimal notation, which has the same format as an IP address. **However, an AreaID is *not* an IP address and bears no necessary relationship to those present.**

There are several advantages of OSPF's area-routing capabilities:

- The use of areas greatly reduces the amount of routing information traffic that must be propagated throughout the entire AS
- Areas allow the development of a hierarchy of routing information, and thus protect each area from external routing information
- The area's information is hidden from routers outside the area. This information-hiding technique is important from a security standpoint, because it prohibits other areas from identifying the physical topology of an area

Every area has its own link-state database consisting of router-LSAs and network-LSAs describing how the area's routers and segments are connected.

In an Extreme Networks configuration (and as defined by the OSPF protocol), AreaIDs are described with 'dotted-decimal notation'. This means Area 0.0.0.1 can be referred to as Area 1, but that Area 0.0.1.0 would therefore equate to Area 256!

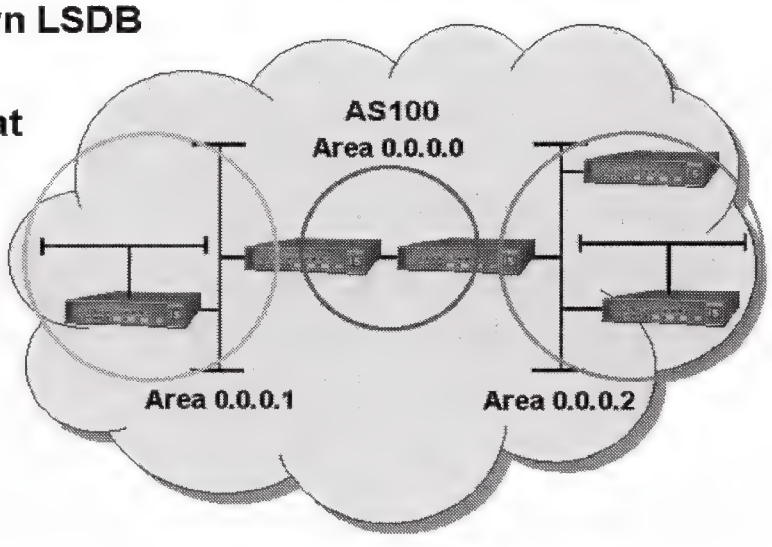
Routers connected to more than one area have a LSDB for each area they are connected to.

Routing within an area is **flat**. In intra-area routing the packet is routed solely on information obtained within the area; no routing information obtained from outside the area can be used. This protects intra-area routing from the injection of bad routing information from outside the area.

© 2001 Extreme Networks,Inc. All rights reserved

OSPF Areas

- Each Area consists of network segments interconnected by routers
- Each Area has a 32-bit address
- Each Area maintains it's own LSDB
- Routing within an Area is flat



Notes:

Area Topology

Detailed knowledge of an area's topology is hidden from other areas in the overall AS. LSAs are not sent between Areas. If you want to connect an area with another area, you have to use a router that has interfaces that are members of both areas. These are known as Area Border Routers (ABR) and are discussed later.

The topology of a network often dictates the type of Area, but all inter-area traffic will be routed through an ABR.

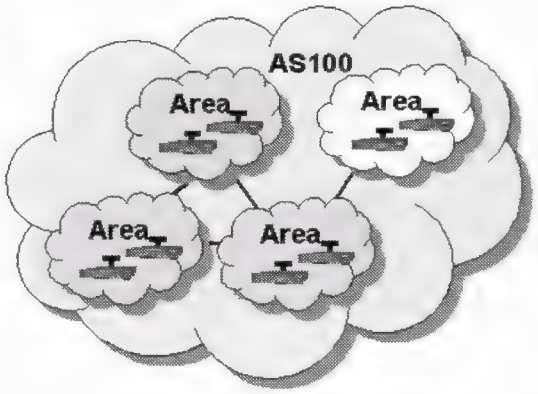
Within an AS there are two basic types of area:

- Normal / Transit Area – IP traffic is able to enter from one Area, pass through the Area and exit to another.
- Stub Area – IP traffic originating from within the area but destined for a network not in the area, has no choice as to how to exit the area – there is only a default route to another area.

© 2001 Extreme Networks,Inc. All rights reserved

Area Topology

- **Detailed knowledge of Area's topology is hidden from all other Areas in the parent AS**
- **Router Link State Advertisements in an Area are not flooded beyond the Area's borders**
- **There are 2 basic types of Areas:**
  - Normal/Transit
  - Stub



Notes:

OSPF Areas - Normal Area

Normal and Transit Areas connect to other areas via ABRs. External routes are distributed into and out of normal areas. These areas are capable of carrying data traffic that is neither locally originated nor locally destined.

- Virtual links (covered later) can be configured through Normal Areas
- A Normal Area is an area that is not a Stub Area or a NSSA (Not-So-Stubby-Area).

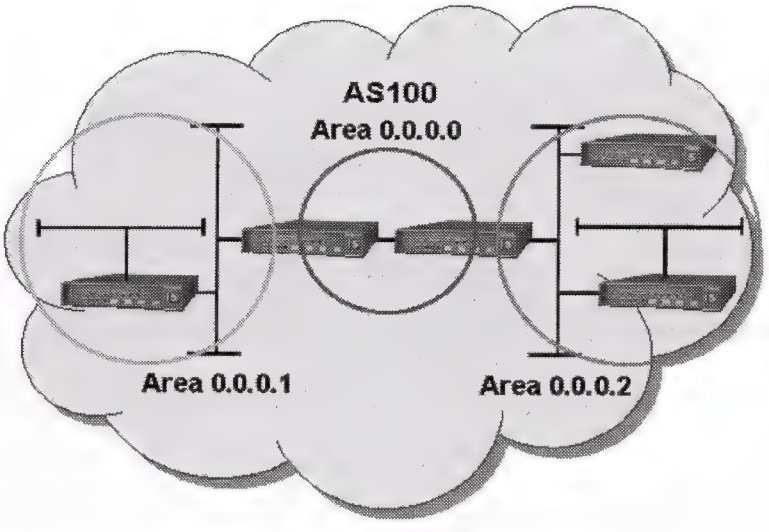
All these new features are detailed in the following pages.

Routers in a Normal Area need to learn about external routes so that they can decide on the best route possible (if there are more than one) to an external network, via an ABR.

© 2001 Extreme Networks,Inc. All rights reserved

OSPF Areas - Normal Area

- Distributes external routes
- Supports Autonomous System Boundary Routers
- Support Virtual Links
- Bounded by Area Border Routers, ABR



Notes:

Area 0 *(Backbone)*

Any OSPF network that contains more than one area is required to have an area configured as Area 0.0.0.0 (referred to as Area 0) which is also called the ***Backbone***. All areas in an Autonomous System (AS) must be connected to the backbone physically via a ABR, or logically via a Virtual Link. When designing networks, you often start with Area 0, and then expand into other areas.

The backbone allows summary information to be exchanged between ABRs. Every ABR hears the area summaries from all other ABRs. The ABR then forms a picture of the cost to all networks outside of its area by examining the collected advertisements, and adding in the backbone cost to each advertising router. The topology of the backbone is invisible to its attached areas, and the topology of the areas is invisible to the backbone.

Inter-area Routing
When routing packets between two areas, the backbone is used. The path that a packet travels can be broken up into three contiguous pieces:

- An intra-area path from the source host to it's areas ABR (connected to the backbone, Are 0.0.0.0)
- A backbone path between the ABRs connected to the source and destination areas
- An intra-area path from the destination ABR to the destination host

The routing algorithm finds the three paths that have the least cumulative cost.

Within an Extreme Networks environment, when a VLAN is configured to run OSPF, by default it is automatically joined to the backbone area (0.0.0.0). If you want to configure the VLAN to be part of a different OSPF area, use;

CLI Command - config ospf vlan
config ospf vlan <vlan name> area <areaid>

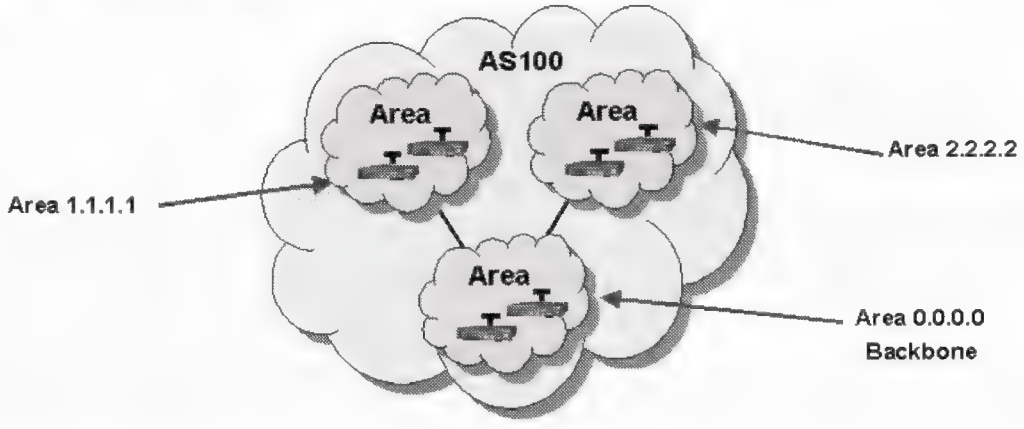
If this is the first instance of the OSPF area being used, you must create the area first, using the following CLI command:

CLI Command - create ospf area
create ospf area <areaid>

© 2001 Extreme Networks,Inc. All rights reserved

Area 0 (*Backbone*)

- Has an Area ID of 0.0.0.0
- Normally the first OSPF Area created and is always a Normal Area
- Only one exists per Autonomous System – as for all Areas
- Responsible for distributing routing information between Areas via ABRs
- Consist of all ABRs, ASBRs and Internal routers (defined later)
- All ABRs are required to attach to the OSPF *backbone* Area either directly or via a Virtual Link



Notes:

Stub Area

OSPF allows certain areas to be configured as "*stub areas*". A stub area is normally connected to only one other area. The area that connects to a stub area must be the backbone area either directly, or indirectly. External route information (i.e. concerning available networks in other areas) is not distributed into stub areas. Stub areas are used to reduce memory and computation requirements on OSPF routers.

In normal practice, AS-external-LSAs (i.e. concerning available networks in other ASs) are not flooded into/throughout stub area - routing to AS external destinations in these areas is based on a (per-area) default only. This reduces the link-state database size, and therefore the memory requirements, for a stub area's internal routers.

In order to take advantage of the OSPF stub area support, default routing must be used on all routers within the stub area. This is accomplished as follows; One or more of the stub area's area border routers must advertise a default route into the stub area via summary-LSAs. These summary defaults are flooded throughout the stub area, but no further (for this reason, these defaults pertain only to the particular stub area). These summary default routes will be used for any destination that is not explicitly reachable by an intra-area or inter-area path (i.e., AS external destinations).

An area can be configured as a stub when there is a single exit point from the area, or when the choice of exit point need not be made on a per-external-destination basis.

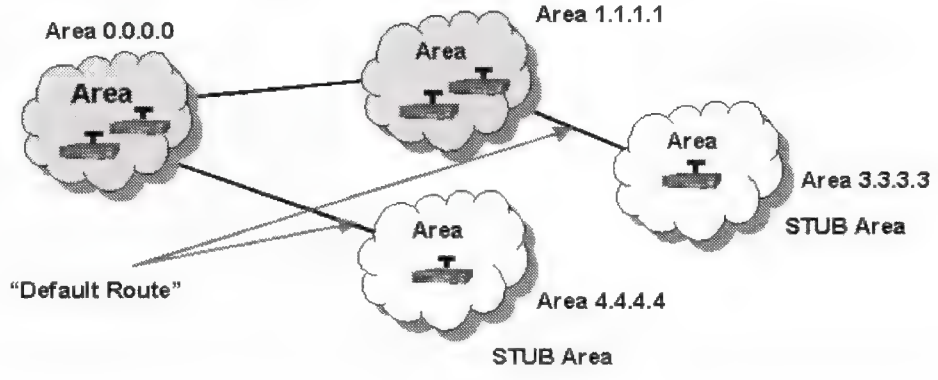
The OSPF protocol ensures that all routers belonging to an area agree on whether the area has been configured as a stub. This guarantees that no confusion will arise in the flooding of AS-external-LSAs.

There are a couple of restrictions on the use of stub areas; virtual links cannot be configured through stub areas and AS boundary routers cannot be placed internal to stub areas.

© 2001 Extreme Networks,Inc. All rights reserved

Stub Area

- **For routers with limited resources**
  - Reduced memory and computation requirements
- **The LSDB is kept as small as possible**
- **External (to the area) route information is not distributed**
  - Will use default routes to ABRs instead
- **Does not support ASBRs**
- **Does not support virtual links**
- **Appears to lie on the edge of an OSPF domain (AS) in configuration**



Notes:

Not-So-Stubby-Area (NSSA)

NSSAs are similar to the existing OSPF stub area configuration option, but have the following two additional capabilities:

- External routes originating from an ASBR connected to the NSSA can be advertised within the NSSA
- External routes originating from a ASBR connected to the NSSA can be propagated to other areas, including the backbone area

NSSAs are an enhancement to current OSPF stub area functionality that allows importing external routes into the stub area and also propagates them out to the rest of the OSPF domain in a limited fashion.

LSA types are discussed later but their use in NSSA is detailed below.

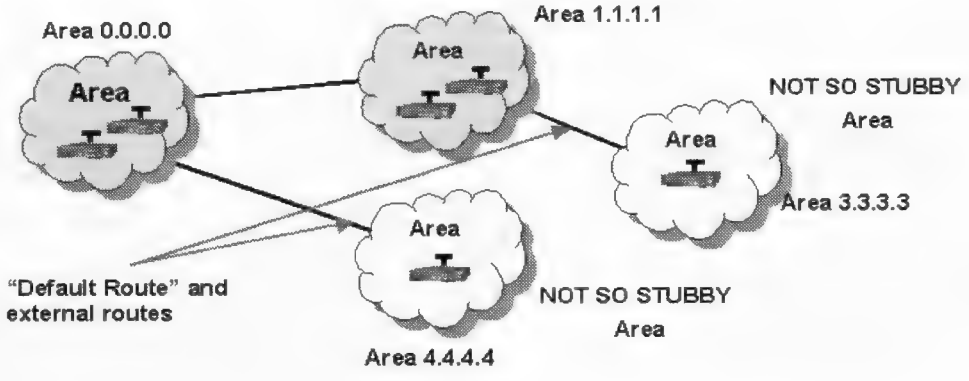
- To support NSSAs, a type of External LSA (Type 7) is defined. The Type 7 LSAs propagate the external link information throughout the NSSA.
- Type 7 LSAs are advertised only within a single NSSA; they are not flooded into the backbone area or any other area by ABRs.
- In order to allow limited exchange of external information across an NSSA area border, NSSA border routers will translate selected Type 7 LSAs received from the NSSA into Type 5 LSAs.
- These Type 5 LSAs will be flooded to all Type 5 capable areas (which does not include Stub Areas)

It should also be noted that unlike stub areas, all OSPF summary routes (Type 3 LSAs) must be imported into NSSAs. This is to ensure that OSPF internal routes are always chosen over OSPF external (Type 7) routes.

© 2001 Extreme Networks,Inc. All rights reserved

Not-So-Stubby-Area (NSSA)

- **Similar to existing OSPF Stub Area with two additional capabilities**
  - External routes originating from ASBR connected to NSSA can be advertised within the Area
  - External routes originating from an ASBR connected to an NSSA can be propagated to other Areas, including the backbone Area.



Notes:

OSPF Router Types

Within the OSPF hierarchy we have defined different types of area. Routers that perform the interconnection of these areas require additional functionality, which gives us 3 types of router:

Internal Router (IR)

- Has all of its interfaces within the same area

Area Border Router (ABR)

- Has interfaces in multiple areas
- Responsible for exchanging area summary advertisements with other ABRs

Autonomous System Boundary Router (ASBR)

- Acts as a gateway between OSPF and other routing protocols (such as RIP), or other Autonomous Systems
- Responsible for generating AS-external-LSAs

To confuse the issue further, within a broadcast network (eg. Ethernet), any of these routers' interfaces can also be designated as:

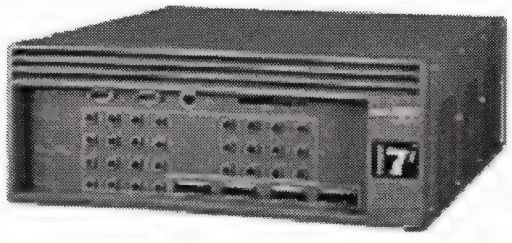
- DR – Designated Router
- BDR – Backup Designated Router
- ODR – Other Designated Router (not a DR or BDR)

These are discussed in detail on the following slides.

© 2001 Extreme Networks,Inc. All rights reserved

OSPF Routers Types

- **Internal Router (IR)**
  - Has all of its interfaces within the same Area
- **Area Border Router (ABR)**
  - Has interfaces in multiple Areas
  - Responsible for summary advertisements with other ABRs
- **Autonomous System Boundary Router (ASBR)**
  - Acts as a gateway between OSPF and other routing protocols
  - Responsible for generating AS-external LSA's
- **Any of the router's interfaces can also be divided into the following types:**
  - DR – Designated Router
  - BDR – Backup Designated Router
  - ODR – Other Designated Router



Notes:

DR - Designated Router Types

OSPF routers exchange link state information with their adjacent neighbours. Because broadcast networks may have many routers, a great deal of bandwidth can be consumed by the routing protocol traffic. Additionally, a broadcast network is able to support the transmission of a single message that is received by a set of defined destinations (multicast).

To reduce this amount of traffic, every broadcast network has a Designated Router (DR) which "represents" all routers on the network, and a Backup Designated Router (BDR).

Essentially, a DR is responsible, on a particular b/c network, for creating a correct LSDB (picture of the area) and ensuring that all other routers on that network have the same LSDB.

Each router on the network exchanges link state information (synchronises databases and forms an adjacency) only with the DR and BDR. This is performed with packets using the special Multicast address 224.0.0.6.

Point-to-Point links do not elect DR or BDR. A router with a priority (which is configurable) of 0 will never be elected DR or BDR.

DR Election

After initalising the OSPF interfaces, the router will send out Hello packets and listen to receive Hello packets for as long as its Wait Timer has defined (normally 4 times the Hello interval which in turn is often 10 seconds). After this time, **if no DR is seen**, the router with the highest configured router priority, or the same priority and highest router ID, will be elected the DR for a network.

The parameters for each router should be configured so that the most dependable router on the network becomes the DR, but that it is not a router that is "very busy" processing a high volume of IP traffic, or already acting as an ASBR, for instance.

The BDR is elected at the same time as the DR. The router with the second highest router priority and router ID is elected the BDR. The BDR reduces the length of time that transit traffic would be disrupted should the DR fail.

The DR will then generate an LSA LS Type 2 - Network-LSAs that:

- Describe a network segment - along with the IDs of all currently attached routers
- Propagate it to all routers in the area

These routers are elected by the use of the Hello protocol that is discussed later.

© 2001 Extreme Networks,Inc. All rights reserved

DR- Designated Router Types

- **To reduce the amount of LSA traffic, a single designated router (DR) and a backup designated router (BDR) are elected on each broadcast domain.**
  - Router LSAs are exchanged only with the DR and the BDR.
  - The router with the highest configured router priority is elected the DR for a network. This should be configured so that the most dependable router on the network becomes the DR.
  - The BDR is elected at the same time as the DR. The router with the second highest router priority is elected the BDR. The BDR reduces the length of time that transit traffic would be disrupted should the DR fail.
  - These are normally the first routers powered up
  - The Designated Router is elected by the Hello Protocol (discussed later)

Notes:

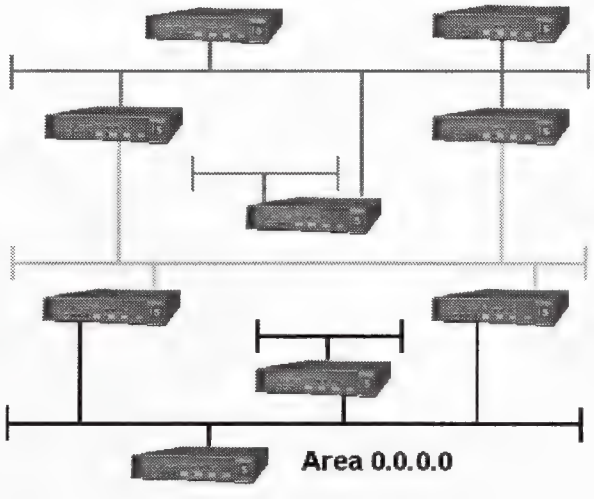
Internal Routers

Internal routers have all of their network interfaces belonging to the same area. IRs run a single copy of the basic routing algorithm and generate a single LSDB.

© 2001 Extreme Networks,Inc. All rights reserved

Internal Routers

- A router with all directly connected networks belonging to the same Area.
- These routers run a single copy of the basic routing algorithm



Notes:

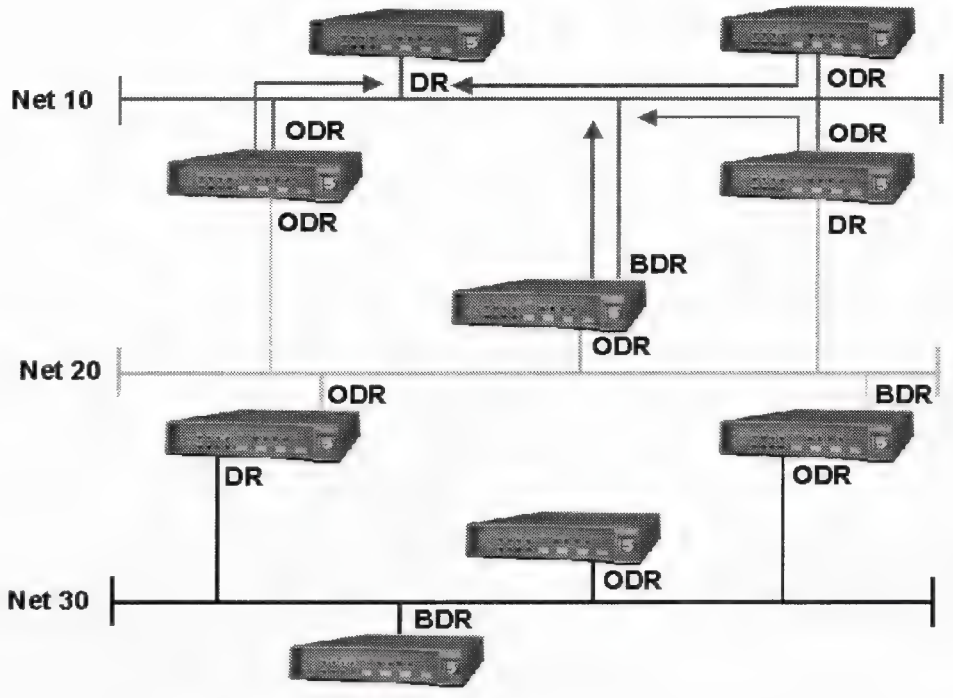
Example Internal Router - Single Area

The diagram shows all the different types of interface that can be configured within a single area. Note that in reality, any router can be configured with interfaces that act as DRs or BDRs, due to loading on the processor, it is normal to ensure (by using the router's priority setting) that only Internal Routers are elected for this role, rather than ABRs, etc.

All routers will send their link state advertisements to the DR on the network segment they are connected to.

© 2001 Extreme Networks,Inc. All rights reserved

Example Internal Router – Single Area



Notes:

Area Border Router (ABR)

An area border router (ABR) is an OSPF router that has interfaces connected to more than one area. ABRs are required to maintain a distinct link-state database, LSBD, for each area and run the SPF algorithm on each area's database.

Because all intra-area traffic **must** cross an ABR, the ABR must always be connected to area 0. This can be achieved logically via a virtual link if a physical connection is not possible or impractical (see later).

An ABR is responsible for summarising the information learned from one area and flooding it throughout all the areas it belongs to in the form of Summary LSAs. As long as the ABR can be reached, the networks that it summarises can be reached. Furthermore, each internal router calculates the cost to reach a summarised network as the sum of the network's Summary LSA cost plus the intra-area cost to reach the ABR. This equates to

Total Cost to destination network = Cost to get across my area to the ABR
+ the cost from the ABR of the n/w

An ABR can originate four different types of LSAs:

- Router LSA (Type 1)
- Network LSA (only if the ABR functions as a DR on a b/c network) (Type 2)
- Summary-Network LSA (Type 3)
- Summary-LSA (ASBR) (Type 4)

These are discussed later.

© 2001 Extreme Networks,Inc. All rights reserved

Area Border Router (ABR)

- **An OSPF router attached to two or more Areas**
  - One Area must be the backbone (Area 0)
  - Attached directly or via Virtual –Link
  - It runs multiple copies of the basic algorithm
  - Manages inter-Area communication
- **Maintains LSDBs for each attached Area**
- **Responsible for condensing the Area's topology information into an LSA for distribution to the backbone.**
  - ***The backbone in turn distributes*** *the information to the other Areas.*
- *As an ABR, each an Extreme switch support up to 8 Areas*

Notes:

ASBR - AS Boundary Router

An autonomous system boundary router (ASBR) is a router that has one or more interfaces in both an OSPF routing domain, and a non-OSPF routing domain such as RIP or BGP. An ASBR is not limited to providing connectivity between one OSPF domain and another autonomous system. An ASBR may provide connectivity between an OSPF domain and a non-OSPF domain in the same autonomous system.

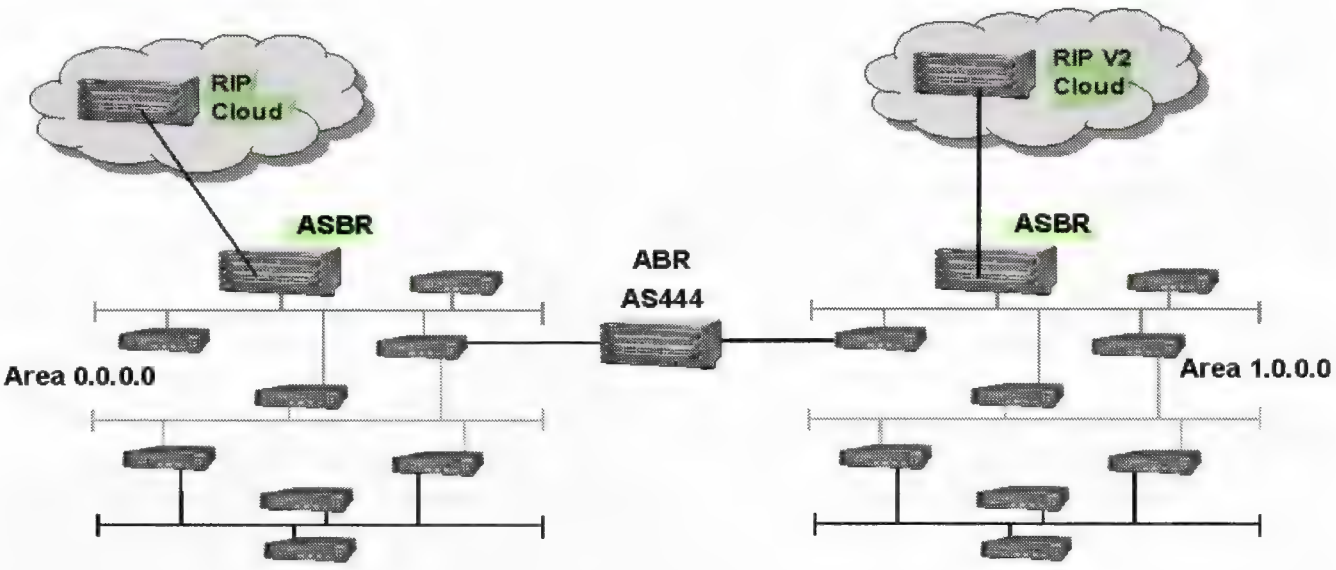
AS External Links Advertisement

An AS External Links advertisement (type 5 LSA) is an LSA originated by ASBRs to describe routes to (external) networks outside the OSPF domain.

© 2001 Extreme Networks,Inc. All rights reserved

ASBR – AS Boundary Router

- An OSPF router that connects to two or more Autonomous Systems (AS)



Notes:

Concept of Virtual Links

OSPF requires that all areas attach directly to the backbone area but not that the attachment be physical. Virtual links will tunnel the summary-LSAs across non-backbone areas, logically maintaining the desired hub and spoke topology for inter-area routing exchange.

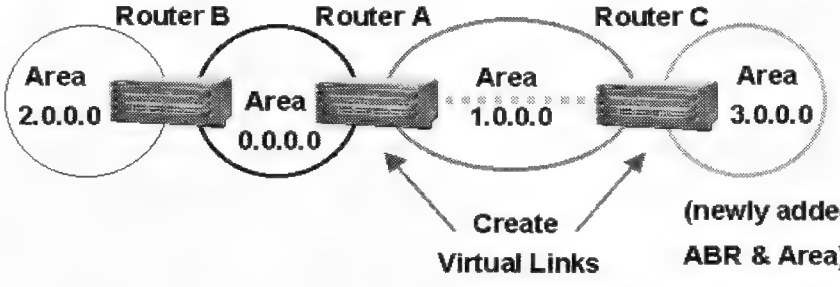
In the situation when a new area is introduced that does have a direct physical attachment to the backbone, a *virtual link* is used. A virtual link provides a logical path between the ABR of the disconnected area and the ABR of the normal area that connects to the backbone. A virtual link must be established between two ABRs that have a common area, with one ABR connected to the backbone. This gives the system administrator control over the routes taken by inter-area traffic.

For example:
Traffic from Area 3 to a network in Area 2will be routed first to the ABR Router C and then directly to ABR Router A. It is then routed through the backbone Area 0 to the ABR Router B, and on through Area 2 to the destination network.

© 2001 Extreme Networks,Inc. All rights reserved

Concept of Virtual Links

- **Used when a new ABR is introduced that does not have a direct physical attachment to the backbone**
  - Recommended only as an interim solution
- **Provides a logical path between the ABR of the disconnected Area and the backbone (Area 0)**
  - It is established between two ABRs (A&C) having a common Area 1, provided that one of the ABRs is connected to Area 0



dont have config virtual Links inbetween.

Notes:

Exercise - Identify OSPF Components

Identify the different area and router types in the network topology presented on the opposite slide. Please complete the following:

Q 1. What do the clouds represent?

Q 2. What possible types of areas can A0 – A4 be?

A0

A1

A2

A3

A4

Q 3. Which area(s) can be Normal, Stub, NSSA?

Normal

Stub

NSSA

Q 4. Do you find anything in the topology that needs to have a virtual link?

Q 5. What are the different types of routers that you find per area?

Q 6. Which are identified as Internal Routers, ABR, ASBR?

IR

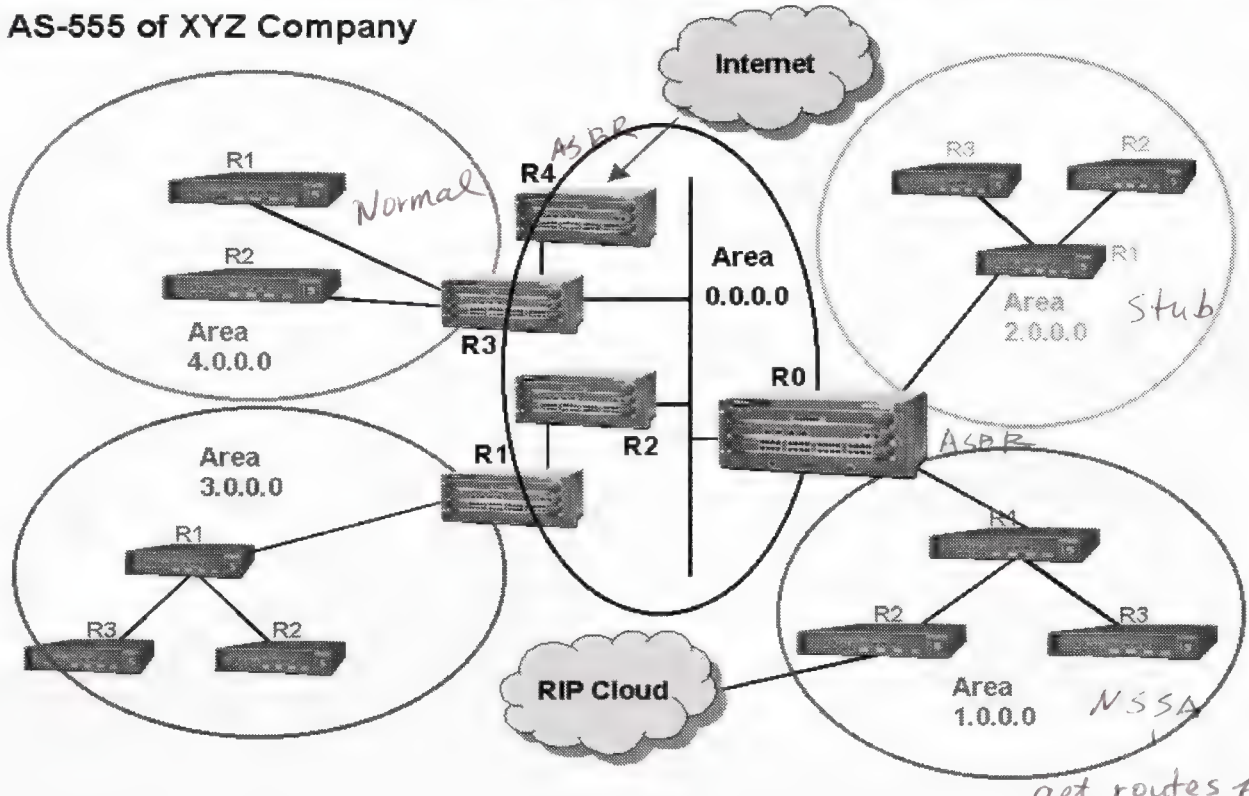
ABR

ASBR

© 2001 Extreme Networks,Inc. All rights reserved

Exercise – Identify OSPF Components

AS-555 of XYZ Company



Notes:

How OSPF Operates

OSPF has been designed to be as resource efficient as possible and one of the several ways of achieving this is in the use of Multicast packets where they are supported. Two multicast addresses/groups are used:

- 244.0.0.5 for all OSPF routers to receive
- 244.0.0.6 for only DR/BDR routers to receive

To understand OSPF operations, let us look at a newly configured OSPF router's perspective. When joining an OSPF network for the first time, the router will undergo several stages prior to actually participating in forwarding/routing of packets. These include the "announcement" of itself, forming adjacencies with neighbours; exchanging information with other routers about the state of it's links and learning about others, etc.

The basic Features of OSPF can be understood by considering the following packets and procedures:

- Hello Packets
- Link State Advertisements (LSA)
- Link State Database (LSDB)
- Reliable Flooding
- Shortest Path First Routing Calculations
- Areas and Inter-area Routing

© 2001 Extreme Networks,Inc. All rights reserved

How OSPF Operates

Newly Configured OSPF Router's Perspective

- Use of IP Multicast packets (224.0.0.5/6)
- Neighbor Discovery & Hello Packet exchange
- DR election occurs
- Initialise LSDB via LSA Exchange
- Synchronise LSDBs and update LSAs through "Reliable Flooding"
- Calculate and build the OSPF Routing table
- Forwarding and Routing Occurs

Notes:

OSPF Router Neighbour Discovery - Hello packet

A router discovers neighbours by sending OSPF Hello packets out of all of its interfaces using m/c group 224.0.0.5. By default, a router sends Hellos out of an interface every 10 seconds. A router learns the existence of a neighbouring router when it receives the neighbour's OSPF Hello in return.

Consider R1 in the diagram: When R1's interfaces first initialise, it would send out its Hello packet to both these interfaces in the hope of receiving a Hello back from any other "listening" routers (in this case R2, R3 and R4).

Once a neighbour has been established, failure of this neighbour (or a link to it) is detected when a router does not receive a Hello from a neighbour within 40 seconds. This timer is called the Router Dead Interval and is configurable

The Hello protocol ensures that neighbour routers agree on timing parameters and can aid in link failure detection. A fault is usually detected way before this time, however, by the data-link protocol since the absence of Hello packets is most likely caused by an interface going down.

"Detecting neighbour failures in a timely fashion is crucial to OSPF protocol performance." (RFC 2178)

By examining the Hello packets received and locating its own listing, a router can be assured that bidirectional communication has been established with all neighbours. Concurrently, the DR and BDR are elected, based on the router priority value. The relationship is now bidirectional and adjacency begins to be set up.

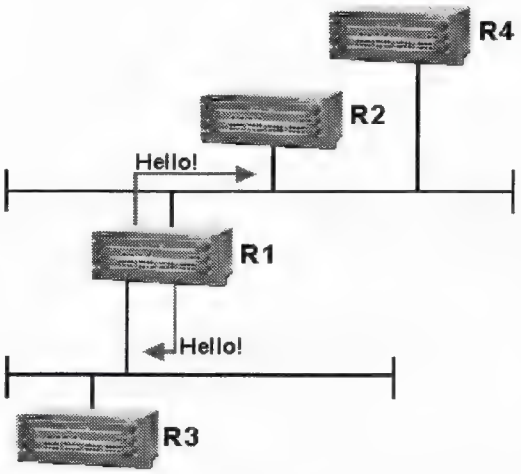
Note that once a router's LSDB is complete and stable, a router will only transmit short, periodic Hello messages until, generally, it is determined that the database is out of date (a change has been detected). This is unlike RIP which periodically broadcasts it's entire routing table.

© 2001 Extreme Networks,Inc. All rights reserved

OSPF Router Neighbour Discovery

Hello Packet

- **Hello packets are sent out on all of a router's interfaces to advertise itself to other routers every 10 seconds by default**
- **A router learns about its neighbours when it receives a neighbour router's Hello packet**
- **Once router neighbours are discovered, subsequent Hello packet are expected within 40 seconds**
  - Otherwise, it will terminate neighbour relationship
- **Neighbors are said to establish an Adjacency**



Notes:

OSPF Hello Packets continued

The Hello packet contains:

- The router's priority value
- The Hello interval in seconds at which the router sends Hello packets on the given network
- A list of routers from which Hello packets have recently been received
- The router's current choice for the DR and the BDR (a value of zero in these fields indicates that one has not yet been selected.)

Before bidirectional neighbours can become fully adjacent, they must decide on an initial sequence number and which router will be the master. The router with the largest router ID becomes the master and it provides the initial sequence number.

After the master/slave relationship is defined, the master sends database description packets to the slave. Database description packets describe the router's link-state database and consist of a list of abbreviated LSAs in the form of *link-state headers*. A link-state header supplies all the information needed to uniquely identify an individual LSA.

The master sends database description packets (polls) that must be acknowledged by database description packets (responses) from the slave.

Based on the summary received from its neighbour, each router builds a list of requests for LSAs that it needs to bring its own database up-to-date. A router builds this list by comparing its link-state database with the link-state headers received in the neighbour's database description packets.

If the router does not have a particular LSA in its link-state database, or if it determines that its neighbour has a more recent version of an LSA (eg the cost is different), the LSA is added to the request list. Each router will send this list in a link-state request packet to its neighbour.

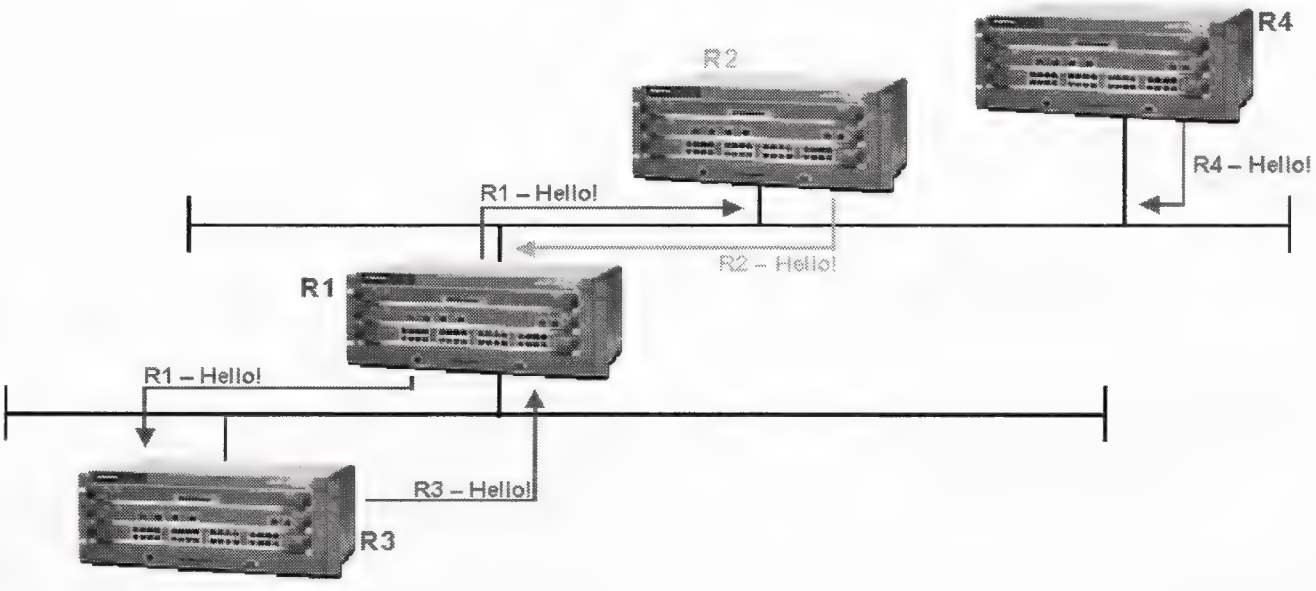
Each router responds to a link-state request packet with a link-state update packet containing the LSAs requested by its neighbour. Neighbours acknowledge the link-state updates with link-state acknowledgment packets. The neighbours become fully adjacent when each has received and acknowledged all requested LSAs.

Once the routers become fully adjacent, they will run the SPF algorithm on the database and add the OSPF routes to their routing tables.

© 2001 Extreme Networks,Inc. All rights reserved

OSPF Hello Packets cont...

- **Ensure that the OSPF link is bi-directional**
  - An OSPF router will not forward data packets over a unidirectional link.



Notes:

Link State Advertisement (LSA)

Each OSPF router is responsible for describing its local piece of the routing topology through the transmission of link-state advertisements. LSAs describe the local state of a router or network. This includes the state of the router's interfaces and adjacencies. Each link state advertisement is flooded throughout the routing domain (area).

Every thirty minutes a router will - even in the absence of any change - re-multicast/retransmit this self-originating data in the event it may have been lost or corrupted in a neighbour router's tables.

The LSA can be of several types:

LSA LS Type 1 - Router-LSAs

- Generated by every OSPF router
- Describes the router's set of active interfaces, their associated cost and any neighbour information
- Flooded throughout a single area only. Link State ID = is the router's OSPF Router ID

LSA LS Type 2 - Network-LSAs

- Generated by OSPF Designated Routers (DRs)
- Describes a network segment - i.e., broadcast domain along with the IDs of all currently attached routers. Link State ID field lists the IP interface address of the DR

LSA LS Type 3 - Summary-LSAs (IP Network)

- Originate from ABRs
- Supports hierarchical routing through the use of OSPF areas. Link State ID field is an IP network number. Type 3 summary-LSAs (IP network) are used when the destination is an IP Network. In this case the LSA's Link State ID field is an IP network number (if necessary, the Link State ID can also have one or more of the network's "host" bits set.

LSA LS Type 4 summary-LSA

- Used when the destination is an AS boundary router and the Link State ID field is the AS boundary router's OSPF Router ID

LSA LS Type 5

- Originated by an ASBR and it describes destinations external to the AS. Link State ID fields specify an IP network number

LSA LS Type 7

- Functionally identical to an LS Type 5 for a Normal Area
- Allows the importation of external routes normally not advertised out of the Not So Stubby Area (NSSA). Destined for ABRs with highest Router ID

LSA types 6 and 8 are currently not supported by Extreme Networks.

© 2001 Extreme Networks,Inc. All rights reserved

Link State Advertisement (LSA)

- **Are transmitted by every OSPF router when neighbour adjacency is established with the DR**
  - LSAs vary according to Link State Types and router function/s
- **Describes a router's local piece of the routing topology that it is responsible for**
- **A router's self-originating LSA is re-transmitted every 30 minutes**
  - Even in the absence of any change, in the event the LSA information may have been lost or corrupted in a neighbour router's tables.
- **Stored in the router's link state database (LSDB)**

Notes:

LSDB Initial Synchronisation

Database synchronisation in a link state protocol is crucial. Synchronisation protects the network as a whole from corrupt information. Of the 5 OSPF protocol packet types, 4 are used for database synchronisation with the Hello packet being the 5th type as follows:

- Link State Request packet
- Link State Update packet
- LS Acknowledge packet
- Database Description packet

Flooding

After a pair of routers becomes fully adjacent, database synchronisation is maintained with a flooding procedure. When an LSA is flooded, it is passed from adjacent router to adjacent router until it has been distributed throughout the entire routing area. LSAs are flooded when the status of a router's links changes or when a timer expires, indicating that it is time for another periodic update.

The decision of any router to pass on the LSA to its adjacent neighbour is based on several conditions. For example, an OSPF router should avoid passing timed-out or self-generated LSAs.

Reliable Updates

OSPF implements a reliable link-state flooding procedure by requiring that the adjacent router acknowledge the receipt and transfer of an LSA. In the absence of an acknowledgment, the source router retransmits the LSA until it is acknowledged or until the adjacency is declared down.

Link-State Age

Every LSA also has an age field, which is used internally to maintain the link-state database. An LSA's age is periodically increased as it is flooded throughout the area and while it resides in a router's link-state database. An LSA can reach an age where it is no longer used in the flooding procedure and must be flushed from the link-state database. Whenever it is determined that there is a change in the link-state database, a new SPT is constructed and the routing table is updated.

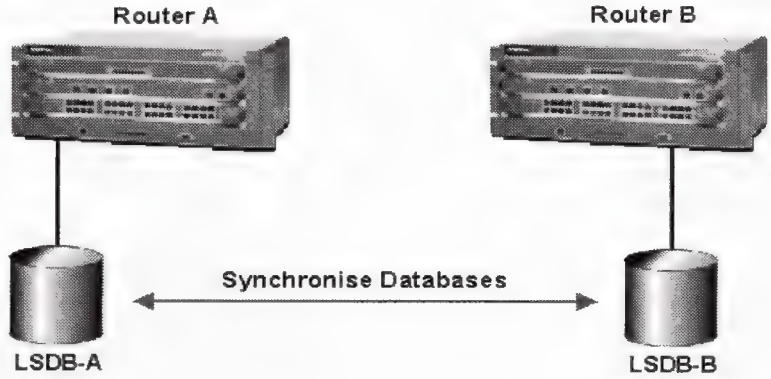
Link-State Sequence Numbers

An LSA in a router's link-state database is often replaced by a more recent LSA from its adjacent neighbour. Each LSA contains a 32-bit sequence number field used by OSPF routers to detect timed-out or duplicate LSAs. A sequence number space is used for LSA identification. When a router generates a new LSA, it uses the next available sequence number. All routers keep their link-state databases synchronised by aging LSAs in their database, and updating with incoming LSAs.

© 2001 Extreme Networks,Inc. All rights reserved

LSDB Initial Synchronisation

- **When two neighbours first start communicating, they must synchronise their databases before forwarding traffic over their shared link to prevent routing loops from occurring**



Notes:

Initialise LSDB - LSA Exchange

The distributed database model shows that every OSPF router has a link state database known as an LSDB. Initially, the only LSA that is found in the router's database is its own LSA.

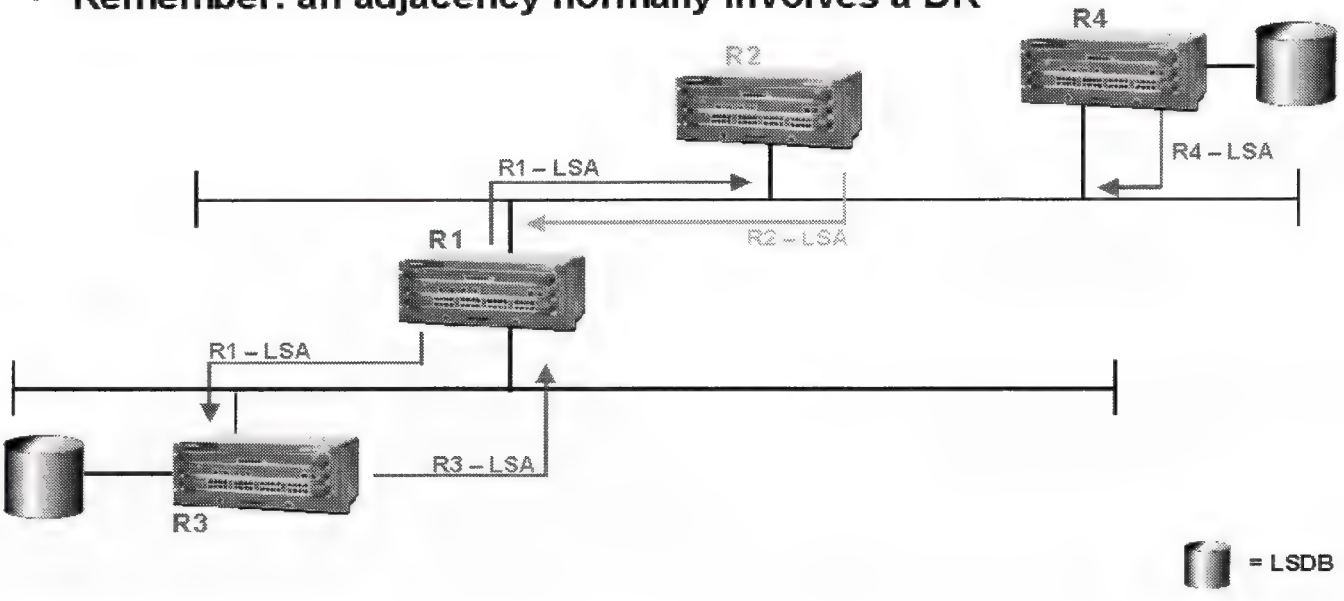
The collection of LSAs is used to form the Link-State Database. Each separate type of LSA has a different function:

- Router LSAs and Network LSAs describe how an area's routers and networks are interconnected
- Summary LSAs provide a way of condensing an areas routing information for transmission to another area
- AS external LSAs provide a way of transparently advertising externally derived routing information throughout the AS

© 2001 Extreme Networks,Inc. All rights reserved

Initialise LSDB - LSA Exchange

- With neighbour adjacency established, routers will exchange LSAs and store them in their LSDBs
- Remember: an adjacency normally involves a DR



Notes:

LSDB Synchronisation

The collection of all OSPF LSAs is called the link-state database. Each OSPF router within an area has an identical link-state database and it gives a complete description of the network including the routers, the network segments, and how they are interconnected.

LSAs are exchanged between neighbouring routers soon after the routers have discovered each other. The link state databases are maintained through a procedure called reliable flooding.

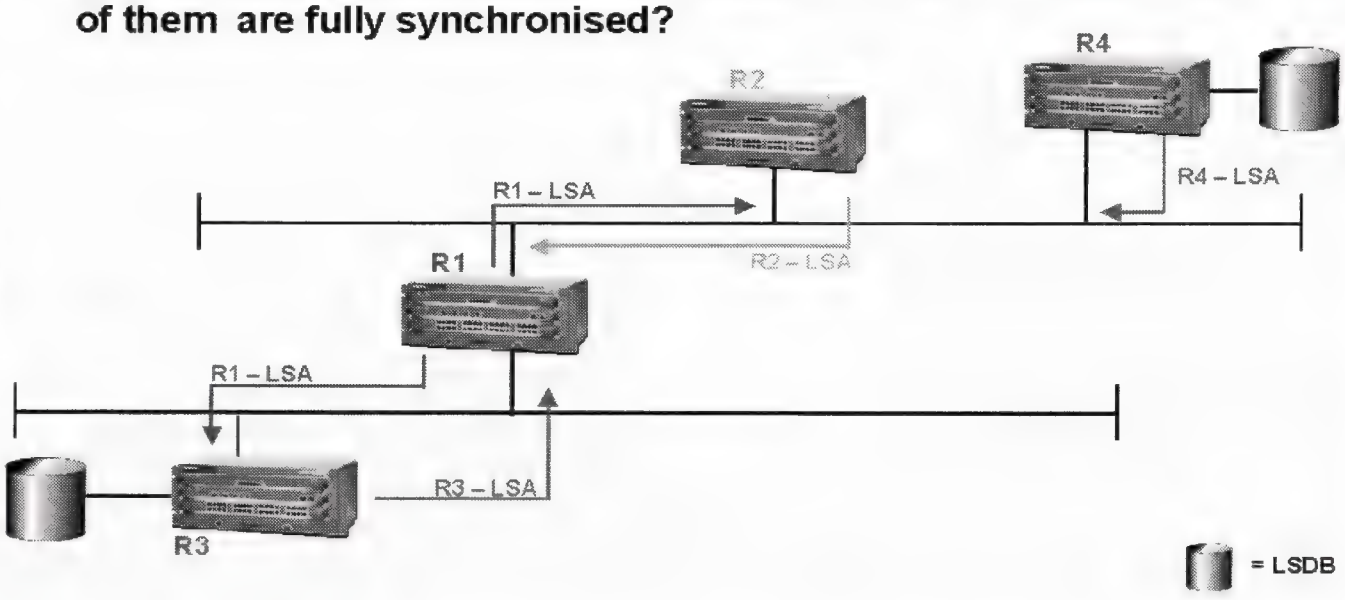
Upon initialisation, each router transmits a link-state advertisement (LSA) on each of its interfaces. LSAs are collected by each router and entered into the Link State Database (LSDB) of each router. OSPF uses flooding to distribute LSAs between routers. Any change in routing information is sent to the DR in the network. These flood the LSA on all interfaces for this area.

All routers within an area have the exact same LSDB.

© 2001 Extreme Networks,Inc. All rights reserved

LSDB Synchronisation

- When all router LSDB contains identical LSAs, they are said to be fully synchronised
- In this example: What will be the contents in each of LSDB if all of them are fully synchronised?



Notes:

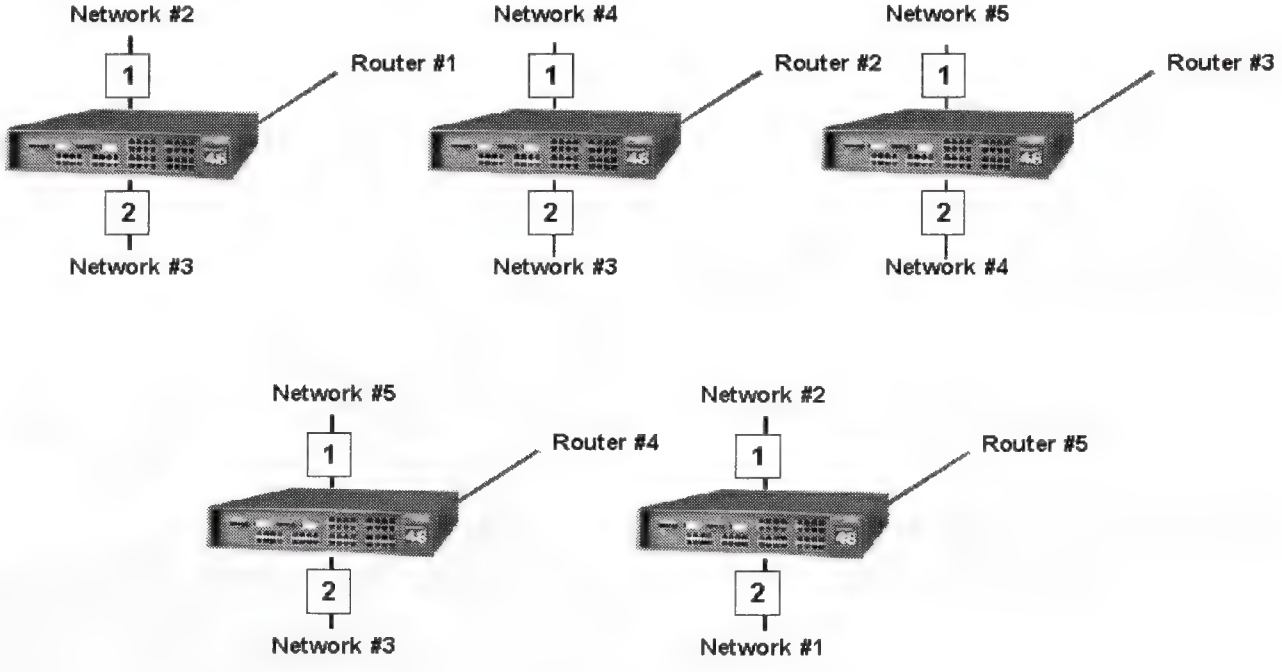
Link State Database

Each router in the domain maintains an identical copy of a database composed of link-state information. The link-state database contains information about the topology of the router's domain, as well as routes to networks outside the router's immediate domain. These external routes may be to networks in a different AS or to networks residing in another area (if the AS is divided into areas).

If a router belongs to multiple areas, it maintains a separate link-state database for each area to which it belongs.

© 2001 Extreme Networks,Inc. All rights reserved

Link State Database



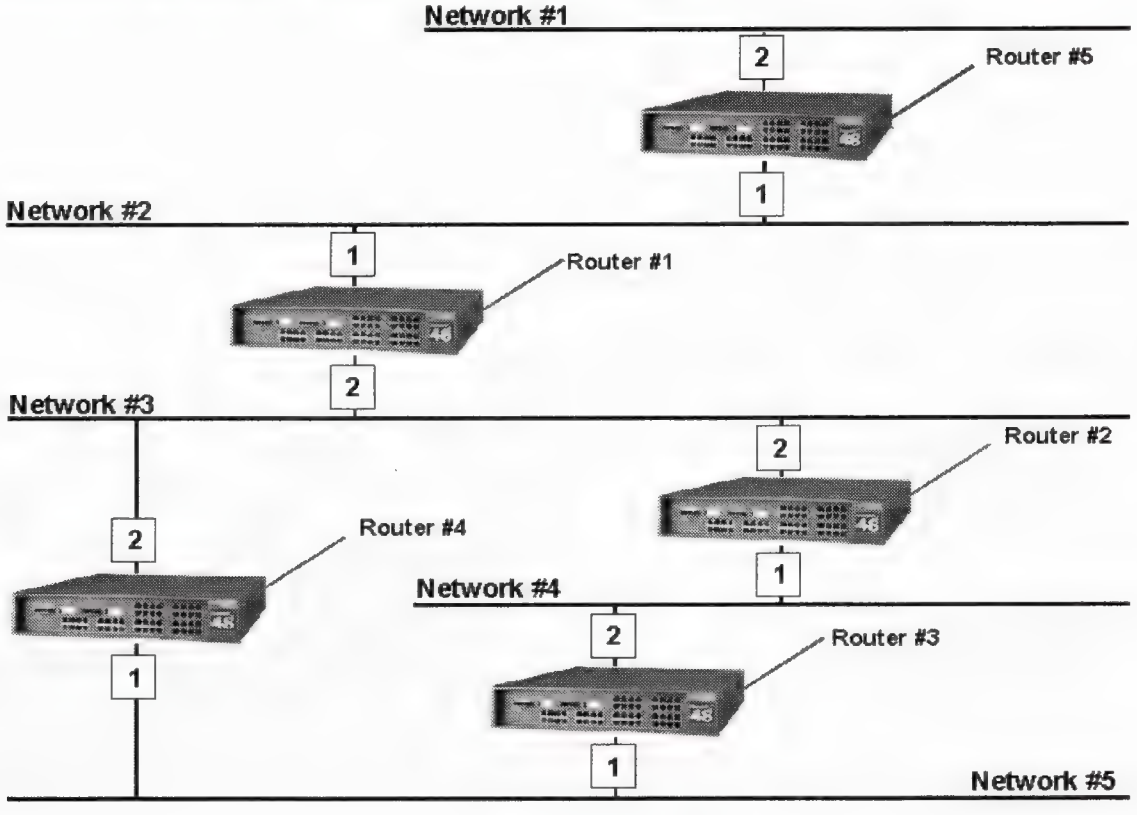
Notes:

Building the Topology Map

The first step in creating a routing table from the link state database is the creation of a topology map. Each router builds a topology map by moving the LSAs around and placing them in the proper position; similar to the way a person would assemble a jigsaw puzzle.

© 2001 Extreme Networks,Inc. All rights reserved

Building the Topology Map



Notes:

Building the Shortest Path Tree

After the topology map is built, each router builds a shortest-path tree (SPT) to all possible destination networks. When building the tree, each router places itself at the root position. The tree is constructed so that the path from the root to each destination network traverses the least-cost path. Notice in our example that the cost from Router 1 to its directly connected networks is 10. However, directly connected networks are entered into the routing table with a cost of zero.

Each router constructs a different SPT despite the fact that all routers are building their trees from an identical link-state database. This is because a router will only appear at the root position of its own tree.

After the SPT is constructed, each router builds its local routing table. From the tree, you can see that Router 1 is directly connected to Network 2 and Network 3. As a result, the routing table shows these networks as directly connected with a cost of zero.

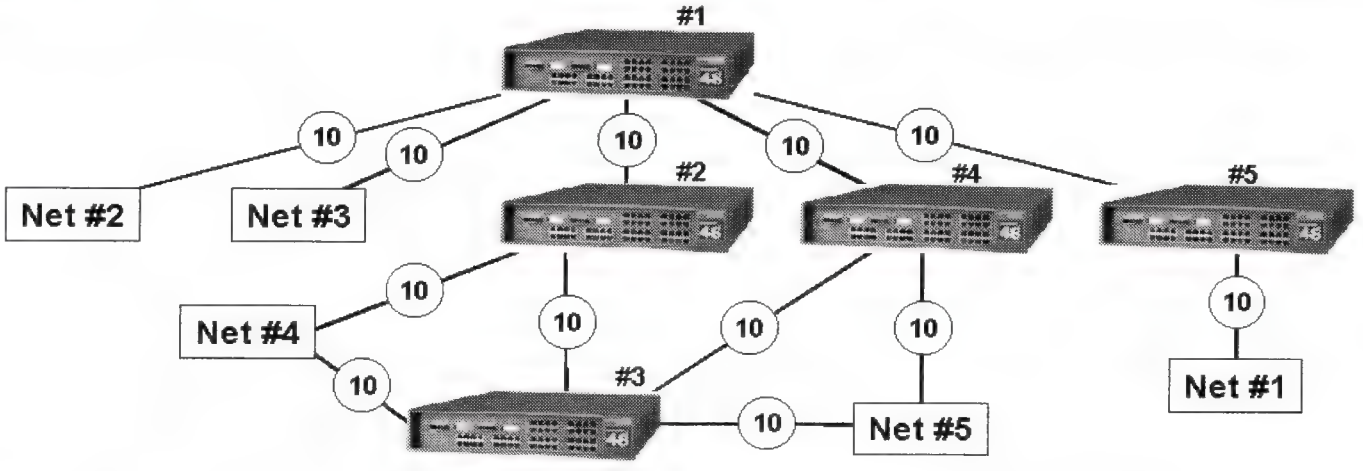
There is a path to Network 1 through Router 5. There is also a path to Network 4 through Router 2. Since the path to each of these networks traverses two branches, the cost entered in the routing table is 20 in both cases.

There are two possible paths to Network 5. One path, with a metric of 30, is through Router 2. The other path has a metric of 20 through Router 4. The link-state routing algorithm will always select the route with the shortest path. As a result, Router 1 selects the route through Router 4.

A similar decision is made regarding Network 4, where the 2 cost comparisons involve via Router 4 at a cost of 30, or via Router 2 at a cost of 20.

© 2001 Extreme Networks,Inc. All rights reserved

Building The Shortest Path Tree



Building the Routing Table for Router 1

Network	Next Hop Router	Metric
Network#1	Router #5	20
Network#2	Direct	0
Network#3	Direct	0
Network#4	Router #2	20
Network#5	Router #4	20

Notes:

OSPF Routing Occurs

It should now be apparent that routing only occurs once:

- OSPF routers establish neighbour adjacency(s), and
- Routers' LSDBs are fully synchronised, and
- Routers' Routing Tables are constructed

Essentially, this is the only point at which the actual IP routing/forwarding engine is able to use any indirect routes.

© 2001 Extreme Networks,Inc. All rights reserved

OSPF Routing Occurs

- After all OSPF routers established neighbour adjacency, and
- Routers' LSDBs are fully synchronised, and
- Routers' Routing Tables are constructed

Notes:

Prior to OSPF Configuration - Things to Consider

- Each router/layer 3 switch that is configured to run OSPF must have a unique router ID
- It is recommended that you manually set the router ID of the switches participating in OSPF, instead of having the switch automatically choose its router ID based on the highest interface IP address. Not performing this configuration in a larger, dynamic environment could result in an older link state database remaining in use and a general lack of control
- If a RouterID changes, its LSAs could stay in the LSDB for 30 minutes. This will corrupt the LSDB for the whole routing domain unless a manual reset is performed
- Virtual links are defined to connect to a specific RouterID. If this target router changes its RouterID the link will fail, possibly isolating an entire area
- **CAUTION**: Do not set the router ID to 0.0.0.0

To configure OSPF for the Extreme Networks switch, you need to learn about the CLI commands. The next section details the CLI commands in question.

© 2001 Extreme Networks,Inc. All rights reserved

Prior to OSPF Configuration

Things to Consider

- **Assign a unique router ID for each switch**
  - The router_ID is normally one of the IP addresses assigned to one of the switch interfaces (VLAN)
- **It is recommended to manually set each OSPF switch's router ID to:**
  - Simplify router management
  - Prevent corruption of virtual links (if applicable)
- **Do not use 0.0.0.0 as a router ID**
  - 0.0.0.0 is used as Area 0's Area ID

Notes:

OSPF Configuration Steps

Before configuring the switch for OSPF operations, it is assumed that the following steps have all been performed:

- Physical cabling for the router connectivity has been done and verified
- The VLANs (router interfaces) for each switch/router have already been created and configured with ports and IP address assigned (see below)

CLI Command – create vlan
create vlan <vlan_name> <cr>
Creates a named VLAN.

CLI Command – configure vlan add ports
configure vlan <vlan_name> add ports <port_list> <cr>
Configures a named VLAN with the specified number or ports.

CLI Command – configure vlan ipaddress
configure vlan <vlan_name> ipaddress <ip_addr> <cr>
Configures a named VLAN with an IP address.

If routing (IP Forwarding) has not already been enabled for all OSPF VLANs:

CLI Command – enable ipforwarding
enable ipforwarding <cr>
Enables IP Forwarding on all configured VLANS.

The CLI commands shown on the slide are explained on the following pages.

© 2001 Extreme Networks,Inc. All rights reserved

OSPF Configuration Steps

- **Configure the router_ID for non-automatic**
  - config ospf routerid <router identifier>
- **Create additional OSPF Areas as required**
  - create ospf Area <Area_id>
- **Configure VLANs for OSPF and assign the Area**
  - config ospf vlan add <vlan_name> Area <Area ID>
- **Enable OSPF globally on the switch**
  - enable ospf
- **Verify configured OSPF parameters**
  - show ospf

Notes:

Basic OSPF CLI Commands

Each of the basic OSPF CLI commands is explained below:

CLI Command – configure ospf routerid
configure ospf routerid [automatic | <router identifier>]

Configures the OSPF router identifier. If "automatic" is specified, the switch uses the largest IP interface address since OSPF was enabled as the OSPF router ID. The default setting is "automatic".

It is **recommended** that you assign your own identifier to the router, as the automatic setting will use the highest IP interface address on the router. It is not necessary for OSPF to be configured on this specific interface, or for the IP interface to be active. There is no requirement for the associated VLAN to be up or have any ports assigned to it.
When the OSPF router-id is set to "automatic" (default), the router-id will be determined by the router every time OSPF is enabled. This means it may change after a reboot, or a disable OSPF command.

CLI Command – create/delete ospf area <area identifier>
create ospf area <area identifier> <cr>
delete ospf area [<area identifier> | all] <cr>

Creates or deletes an OSPF area. Area 0.0.0.0 does not need to be created as it exists by default. It also cannot be deleted. Once an OSPF area is removed, the associated OSPF interface information will also be removed.
CLI Command - config ospf add/del vlan
configure ospf add vlan [<name> | all] area <area identifier> <cr>
configure ospf delete vlan [<vlan_name> | all] <cr>

Enables or disables OSPF on one or all VLANs (router interfaces). The <area identifier> specifies the area to which the VLAN is assigned. The default setting is disabled.

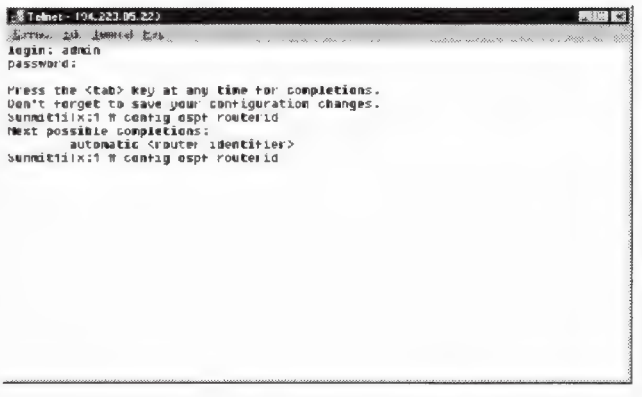
CLI Command - enable/disable ospf
enable ospf <cr>
disable ospf <cr>

This is a global command to enable or disable OSPF processing in the router. The default is "disabled".

© 2001 Extreme Networks,Inc. All rights reserved

Basic OSPF CLI Commands

- **config ospf routerid**
- **create ospf Area**
  - delete ospf Area
- **config ospf add vlan Area**
  - config ospf delete vlan
- **enable ospf**
  - disable ospf



Notes:

Example: show ospf

CLI Command - show ospf
show ospf {[area | ase-summary | interfaces | lsdb | virtual-link]}

Displays global OSPF information. If the following is specified:

- AREA: Displays information about a particular OSPF area, or all OSPF areas.
- ASE-SUMMARY: Displays the OSPF AS external route aggregation configuration
- INTERFACES: Displays information about one or all OSPF interfaces
- LSDB: Displays current LSDB table
- VIRTUAL LINK: Displays virtual link information about a specified router/s

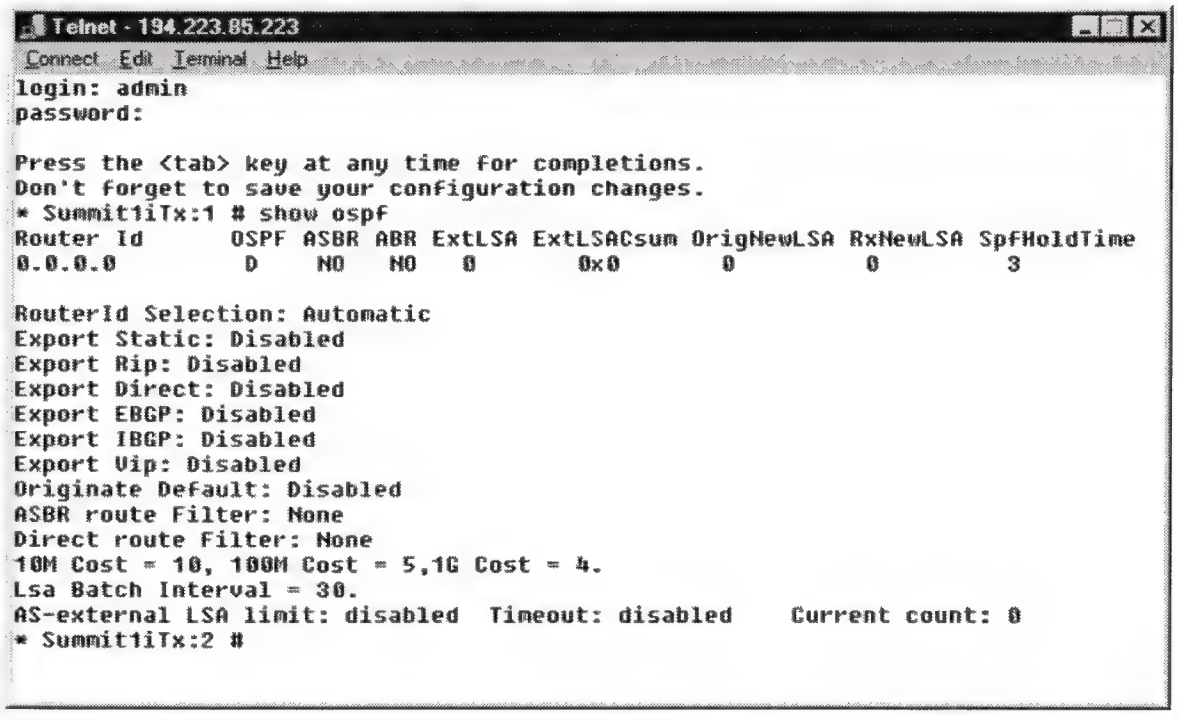
CLI Command - show ospf
Show ospf

Displays the OSPF area information. If no argument is specified, then all the OSPF areas will be shown:

- Area ID, Area Type (stub or normal), and Router ID
- Number of SPF executions, number of ABRs known, number of ASBRs known, number of LSAs in LSDB, and the LSA checksum
- List of router interfaces (VLANs), their OSPF state, the link state, and the router ID for the DR and BDR
- Configured address ranges, if any

© 2001 Extreme Networks,Inc. All rights reserved

Example: show ospf


Telnet - 194.223.85.223
Connect Edit Terminal Help
login: admin
password:
Press the <tab> key at any time for completions.
Don't forget to save your configuration changes.
* Summit1iTx:1 # show ospf
Router Id OSPF ASBR ABR ExtLSA ExtLSACsum OrigNewLSA RxNewLSA SpfHoldTime
0.0.0.0 D NO NO 0 0x0 0 0 3
RouterId Selection: Automatic
Export Static: Disabled
Export Rip: Disabled
Export Direct: Disabled
Export EBGP: Disabled
Export IBGP: Disabled
Export Vip: Disabled
Originate Default: Disabled
ASBR route Filter: None
Direct route Filter: None
10M Cost = 10, 100M Cost = 5,1G Cost = 4.
Lsa Batch Interval = 30.
AS-external LSA limit: disabled Timeout: disabled Current count: 0
* Summit1iTx:2 #

Notes:

Configuring OSPF Virtual Links

Continuing with more OSPF configurations, the following are the commands for configuring virtual-links on Extreme Networks switches.

Virtual links are considered an interim solution to an existing network setup. When a router is to become an ABR for a newly created area and that ABR does not have a direct connection to the area 0, a virtual link is used.

It is configured on the ABR which has a direct connection to area 0, and the ABR that does not have any link to area 0, yet has an interface to the new area created.

There must be a common area shared between these two ABRs that is to be configured with virtual links, known as the transit area.

The ABR virtual link routerid must equal the routerid of the neighbour ABR with a link to the area 0 and vice versa.

CLI Command – config ospf add/delete virtual-link

configure ospf add virtual-link <router identifier><area identifier>
configure ospf delete virtual-link <router identifier><area identifier>

To add a virtual link connected to another ABR. Specify the following:

- Router identifier - Far-end router interface number
- Area identifier - Transit area used for connecting the two end-points. The transit area cannot be the backbone, area 0.0.0.0.

Note: A virtual link cannot be configured through a stub area.

CLI Command – show ospf virtual-link

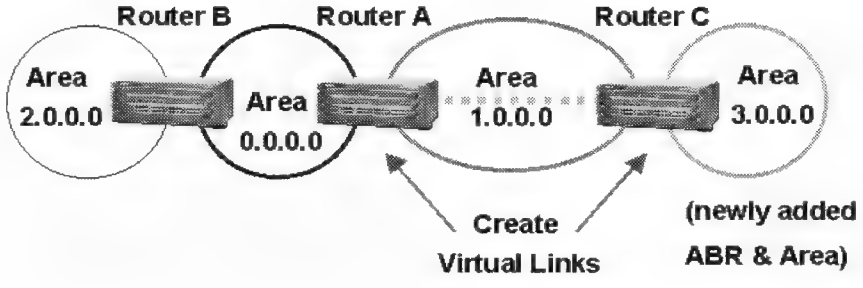
show ospf virtual-link <router identifier>
Display the virtual-link configuration and operation information. Default is all:

- Area ID and neighbour router ID
- Receive interval, transit delay, Hello interval, and dead interval
- Authentication configuration
- Virtual link type and number of events
- Neighbour router ID, IP address, and priority
- Link state, DR ID, BDR ID, and dead time

© 2001 Extreme Networks,Inc. All rights reserved

Configuring OSPF Virtual Links

- **config ospf add virtual-link**
  - config ospf delete virtual-link
- **show ospf virtual-link**



Notes:

Summary

The main theme of chapter ten has been to discuss the IP routing protocol Open Shortest Path First (OSPF), available on the Extreme Networks range of switches. You should now be able to:

- Define OSPF as a routing protocol
- Describe how to build OSPF Networks
- Define OSPF Areas, router types and virtual links
- Describe how OSPF operates
- Define LSA, LSDB, initial synchronisation, database exchange and reliable flooding
- Describe OSPF Configuration and examples
- Successfully complete the lab exercises to follow

© 2001 Extreme Networks,Inc. All rights reserved

Summary

You should now be able to:

- **Define OSPF as a routing protocol**
- **Describe how to build OSPF Networks**
- **Define OSPF Areas, router types and virtual Links**
- **Describe how OSPF Operates**
- **Define LSA, LSDB, Initial synchronisation, database exchange & reliable flooding**
- **Describe OSPF Configuration and Examples**
- **Complete the Lab Exercises**

Notes:

Config ospf area <areaid> nssa [summary | nosummary]
stub-default-cost <cost> & translate?

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 11

ESRP Overview and Configuration

Chapter Objectives

The main theme of chapter eleven is to discuss the Extreme Standby Router Protocol (ESRP) available on the Extreme Networks range of switches.

Upon completion of this chapter, you will be able to:

- Describe ESRP in overview
- Explain the Basics of ESRP
- Describe the Determination of the ESRP Master
- Describe ESRP Tracking Information Options
- Define the Master Election Algorithm choices and when election occurs
- Describe how to configure ESRP
- Provide ESRP Example Configurations
- Successfully complete the ESRP Lab exercises

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

Upon completion of this chapter, you will be able to:

- **Describe ESRP**
- **Discuss the Basics of ESRP and define EDP**
- **Describe the Determination of ESRP Master**
- **Discuss ESRP Tracking Information Option**
- **Define the Master Election Algorithm choices and when election occurs**
- **Describe how to configure ESRP**
- **Provide ESRP Example Configurations**
- **Successfully complete the ESRP Lab exercises**

Notes:

ESRP Defined

ESRP (Extreme Standby Router Protocol) is a feature of ExtremeWare that allows multiple switches to provide redundant routing services to users.

ESRP works by allowing you to configure a virtual router on two or more Extreme Networks switches that are part of the same VLAN. Connected hosts are then configured using the IP address of the virtual router as the default gateway.

ESRP provides both L3 routing and Layer 2 switching redundancy with a single technology. Traditional techniques to achieve a similar level of resilience would require the configuration of separate layer 2 and layer 3 protocols, such as STP and VRRP, increasing overall system complexity.

From the workstation's perspective, there is only one default gateway (that has one IP address and one MAC address) regardless of how many switches are providing the ESRP resiliency. This means that ARP cache entries in client workstations do not need to be refreshed or timed-out, this provides for fast fail-over in the event of a network or hardware problem

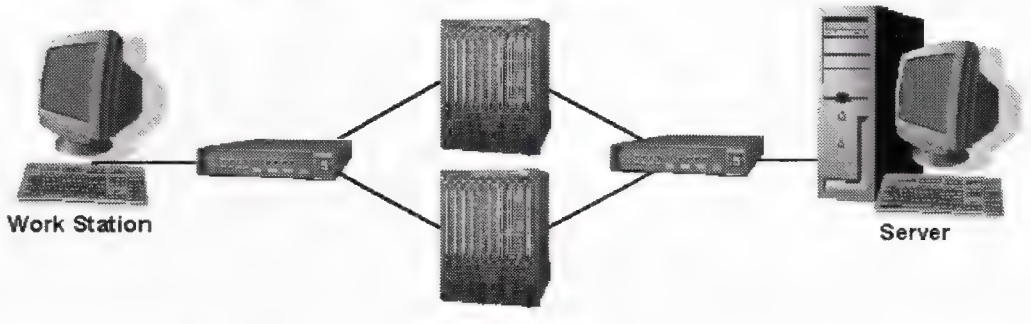
ESRP is primarily used as technique for providing redundancy within the core of a network, however it can also be configured to provide resiliency to end stations, and provide for dual-homed system design.

These "layered" redundancy features can be used in combination or independently. You do not have to configure the switch for routing to make valuable use of ESRP. The L2 redundancy features of ESRP offer fast failure recovery (usually 4 to 9 seconds). ESRP can provide better resiliency than using the Spanning Tree Protocol (STP).

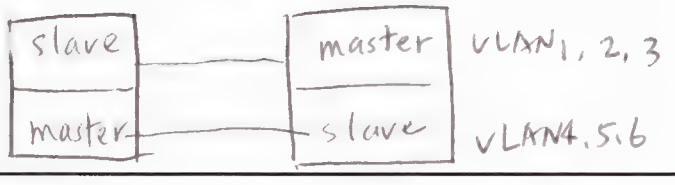
© 2001 Extreme Networks,Inc. All rights reserved

ESRP Defined

- ESRP - Extreme Standby Router Protocol
  - It is an ExtremeWare feature
- **Enables multiple switches to provide routing redundancy at Layer 2 & 3.**
- **Provides a way to keep host communications when a physical router becomes unavailable**
- **Provides better resiliency than STP**
- **Allows you to configure a virtual router on two or more Extreme switches belonging to the same network segment**
- ***ESRP is enabled on a per VLAN basis***



Notes:



ESRP Defined continued

The switches exchange keep-alive packets for each VLAN independently. Only one switch can actively provide layer 3 routing and/or layer 2 switching for each VLAN. The switch performing the forwarding for a particular VLAN is considered the "master" for that VLAN. Other participating switches for the VLAN are in standby mode.

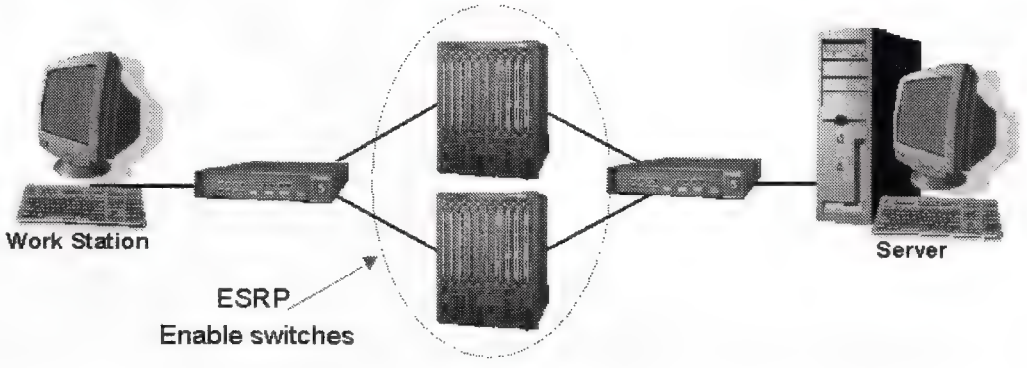
For a VLAN with ESRP enabled, each participating switch uses the same MAC address and must be configured with the same IP address or IPX NetID. It is possible for one switch to be master for one or more VLANs while being in standby for others, thus allowing the load to be split across participating switches.

It is highly recommended all switches participating in ESRP run the same version of ExtremeWare. Not all ESRP features are available in all ExtremeWare software releases.

© 2001 Extreme Networks,Inc. All rights reserved

ESRP Defined cont..

- Only one of the virtual routers (per VLAN) is active at any given time. This is called the *Master* or *active router.*
- The other virtual routers (called Slaves) remain in *standby* mode and do not route packets.
- When an *active router* fails, one of the *Slave* or *standby routers* becomes the *active router.*
- A switch can be the Master and Slave router time for different VLANs at the same



Notes:

ESRP - Aware Switches

Extreme Networks switches that are not running ESRP, but are connected on a network that has other Extreme Networks switches running ESRP are called ***ESRP-aware***. This means that when Extreme Networks switches are attached to the ESRP-enabled switches, the non-ESRP switches reliably perform fail-over and fail-back scenarios in the prescribed recovery times. No configuration of this feature is necessary.

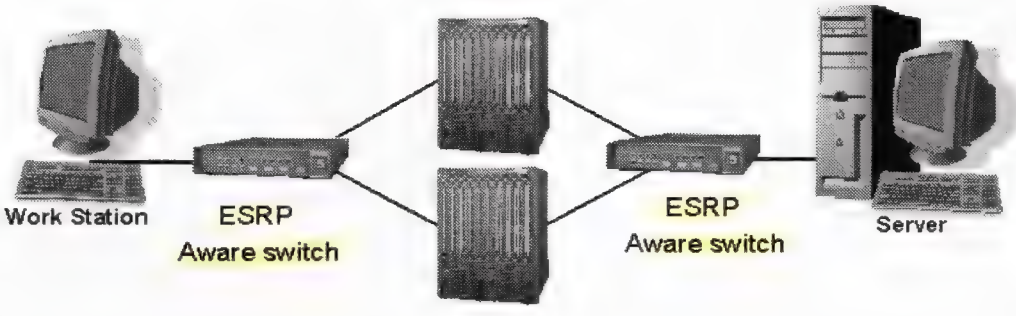
If Extreme Networks switches running ESRP are connected to layer 2 switches that are not manufactured by Extreme Networks (or Extreme Networks switches that are not running ExtremeWare 4.0 or above), the fail-over times seen for traffic local to the segment may appear longer, depending on the application involved and the Forwarding Database (FDB) timer used by the other vendor's layer 2 switch (this is the aging timer for MAC entries). As such, ESRP can be used with layer 2 switches from other vendors, but the recovery times vary.

The VLANs associated with the ports connecting an ESRP-aware switch to an ESRP-enabled switch must be configured using an 802.1Q tag on the connecting port, or, if only a single VLAN is involved, as untagged using the protocol filter **any**. ESRP will not function correctly if the ESRP-aware switch interconnection port is configured for a protocol-sensitive VLAN using untagged traffic.

© 2001 Extreme Networks,Inc. All rights reserved

ESRP-Aware Switches

- These are Extreme Networks switches that are not running ESRP, but are connected on a network with switches running ESRP
- These switches will detect an ESRP master change and flush their forwarding databases
- The command show esrp-aware [vlan <vlan name>] will show related statistics



Notes:

ESRP Basics

A maximum of four ESRP enabled switches can participate in providing redundant layer 3 or layer 2 services to a single VLAN. These switches exchange keep-alive packets for each VLAN independently. Only one switch can actively provide L3 and/or L2 switching for each VLAN.

The switch performing the forwarding for a particular VLAN is considered the "master" for that VLAN. Other participating switches (Slaves) for the VLAN are in standby mode.

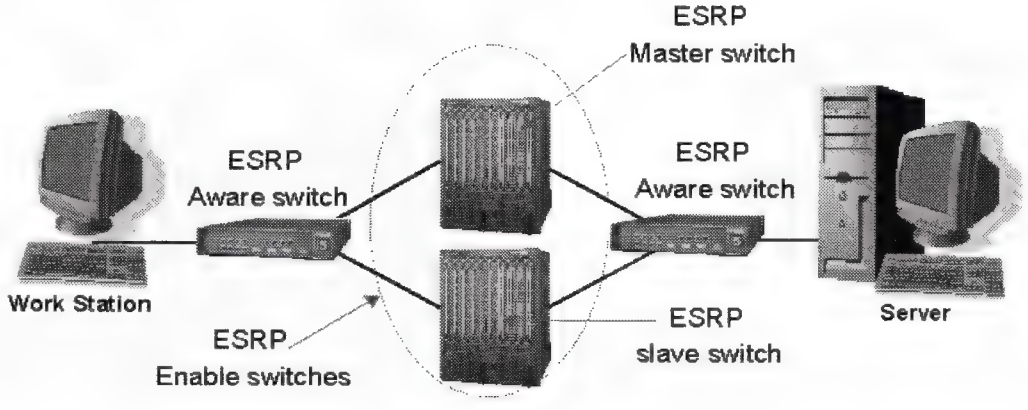
For a VLAN with ESRP enabled, each participating switch uses the same MAC address and must be configured with the same IP address. It is possible for one switch to be master for one or more VLANs while being in standby for others, thus allowing the load to be split across participating switches.

The MAC address is assigned automatically when ESRP is enabled, but the IP address must be configured manually

© 2001 Extreme Networks,Inc. All rights reserved

ESRP Basics

- **ESRP is configured on a per-VLAN basis on each switch**
- **Maximum of four switches can participate in providing redundant layer 3 or layer 2 services to a single VLAN**
  - They must be in the same VLAN (L2 broadcast domain)
  - Only one switch can actively provide L3 and/or L2 switching for each VLAN.
  - The switch performing forwarding for the VLAN is considered the "master".
  - Other participating switches (slaves) are in standby mode.



Notes:

Linking ESRP Switches (Direct Links)

When considering system design using ESRP, direct links between ESRP switches are useful, if not mandatory, under the following conditions:

- A direct link can provide a more direct routed path, if the ESRP switches are routing and supporting multiple VLANs where the master/standby configuration is split such that one switch is master for some VLANs and a second switch is master for other VLANs. The direct link can contain a unique router-to-router VLAN/subnet, so that the most direct routed path between two VLANs with different master switches uses a direct link, instead of forwarding through another set of connected routers. This unique VLAN is not running ESRP

- A direct link can be used as a highly reliable method to exchange ESRP hellos, so that the possibility of having multiple masters for the same VLAN is lessened, should all downstream Layer2 switches fail.

Direct links may contain a router-to-router VLAN, along with VLANs running ESRP. If multiple VLANs are used on the direct links, use 802.1Q tagging. The direct links may be aggregated into a load-shared group, if desired.

- A direct link is necessary when using the ESRP HA option. The direct link is used to provide Layer2 forwarding services through an ESRP standby switch (this is discussed later)

In the example shown, a direct switch link is required to pass information between the two switches.

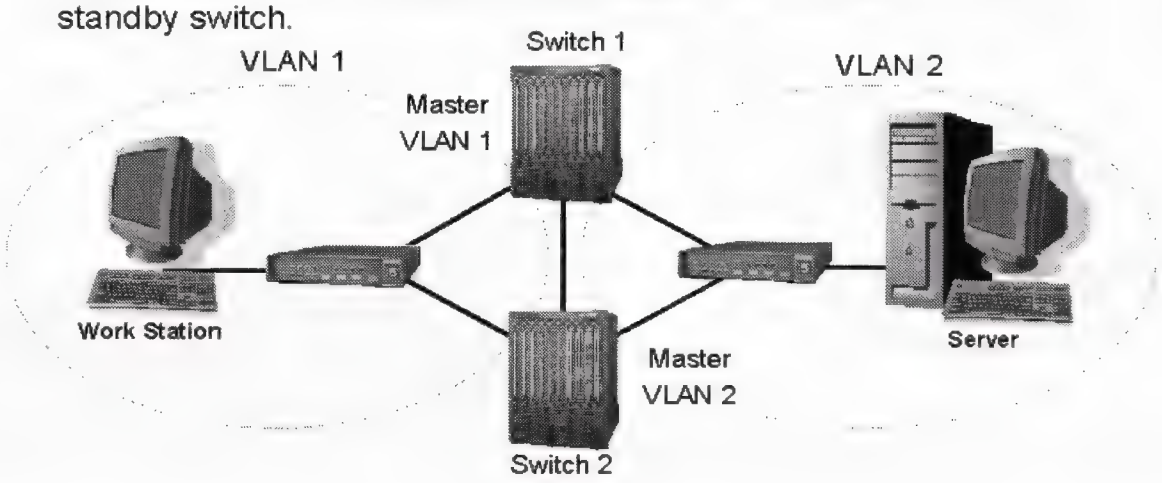
Switch 1 is configured as the Master for VLAN 1. Switch 2 is configured as the Master for VLAN 2. In order to enable IP routing between the two VLANS we need to enable a third VLAN on **BOTH** switches, and the direct link is required to provide connectivity.

ESRP is not running on this link

© 2001 Extreme Networks,Inc. All rights reserved

Linking ESRP Switches (Direct Links)

- **Can provide a more direct routed path**
  - The link can contain a unique router-to-router VLAN/subnet
- **Can be used as a highly reliable method to exchange ESRP hellos**
- **It is necessary when using the ESRP HA option** host attaching
  - It is used to provide Layer2 forwarding services through an ESRP standby switch.



Notes:

Steps for Switches to Perform ESRP

- For each VLAN to be made redundant, the switches must have the ability to exchange packets on the VLAN i.e. they must be on the same Layer 2 broadcast domain. Multiple paths of exchange can be used, and typically exist in most network system designs that take advantage of ESRP.
- In order for a VLAN to be recognised as participating in ESRP, the assigned IP address or the IPX NETid for the separate switches must be identical. Other aspects of the VLAN, including its name, are ignored.
- ESRP must be enabled on the desired VLANs for each switch.
- NOTE: ESRP cannot be enabled on the VLAN default.
- EDP - Extreme Discovery Protocol, must be enabled on the ports that are members of the ESRP VLANs (The default setting is enabled.).

To verify EDP status, use the following;

CLI command - show port <portlist> info
show port <portlist> info <cr>

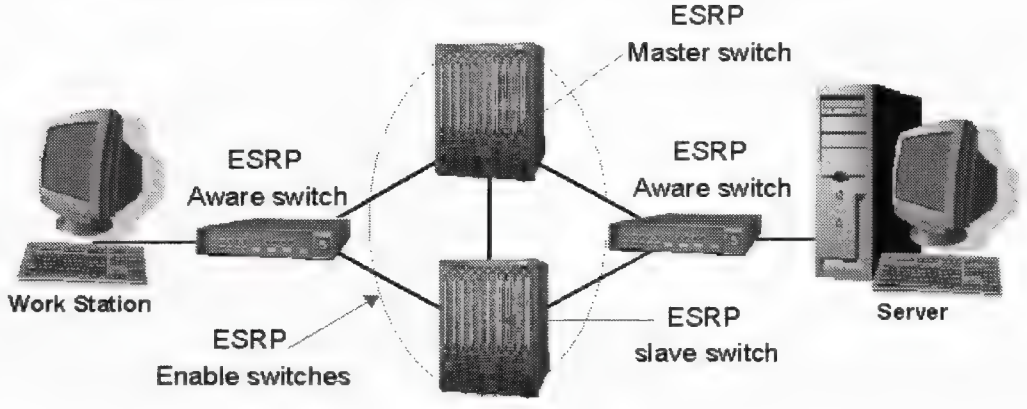
Spanning Tree and ESRP will not work together on the same switch within the same VLAN.

It is highly recommended all switches participating in ESRP run the same version of ExtremeWare. Not all ESRP features are available in all ExtremeWare software releases.

© 2001 Extreme Networks,Inc. All rights reserved

Steps for Switches to perform ESRP

- **Switches must have the ability to exchange packets on the same L2 broadcast domain for the protected VLAN**
- **Assign the same IP address or IPX NETid for each separate switch**
- **Enable ESRP on desired VLANs per switch**
  - *ESRP cannot be enabled on VLAN "default"*
- **EDP must be enabled on ports that are members of ESRP VLANs**
  - EDP - Extreme Discovery Protocol is enabled by default.



Notes:

Extreme Discovery Protocol (EDP) Defined

The Extreme Discovery Protocol (EDP) is used to gather information about neighbour Extreme Networks switches. EDP is used by switches to exchange topology information.

EDP is the protocol that allows switches to run ESRP or be ESRP aware.

Information communicated using EDP includes the following:

- Switch MAC address (switch ID)
- Switch software version information
- Switch IP address
- Switch VLAN-IP information
- Switch port number

EDP Frames are sent out of each port that it is enabled on. These frames are sent at 60-second intervals.

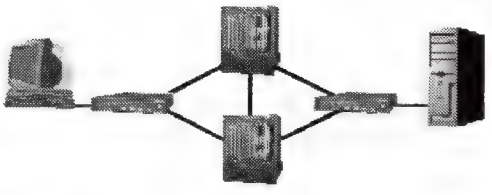
EDP Packets have 2 formats, The General Info PDU and the VLAN Info PDU.

- The General Info PDU is sent at first, if a neighbour switch is seen, then the Neighbours exchange VLAN Info PDU's.

© 2001 Extreme Networks,Inc. All rights reserved

Extreme Discovery Protocol (EDP) Defined

- **The Extreme Discovery Protocol (EDP)**
- **Allows switches to run or be ESRP aware**
- **It is used to gather information about neighbour Extreme Networks switches.**
- **It is used by the switches to exchange topology information which includes:**
  - Switch MAC address (switch ID)
  - Switch software version information
  - Switch SystemName
  - Switch VLAN-IP information
  - Switch slot, port number
  - Checksum, which checks for packet corruption



Notes:

ESRP Switch Behavior

NOTE: A switch can be a master and slave at the same time for different VLANs.

If a switch is master, it actively provides layer 3 routing services to other VLANs, and layer 2 switching between all the ports of that VLAN. Additionally, the switch exchanges ESRP and EDP packets with other switches that are in standby mode.

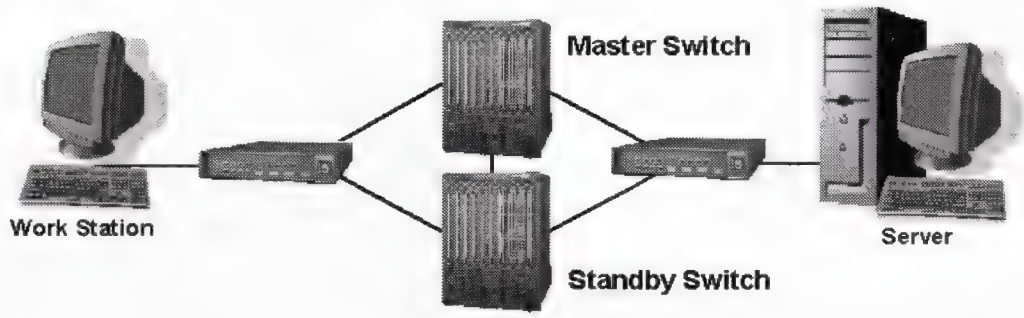
If a switch is in standby mode, it exchanges ESRP packets with other switches on that same VLAN. When a switch is in standby, it does not perform layer 3 routing or layer 2 switching services for the VLAN.

From a layer 3 routing protocol perspective (for example, RIP or OSPF), when in standby for the VLAN, the switch marks the router interface associated with the VLAN as down. From a layer 2 switching perspective, no forwarding occurs between the member ports of the VLAN; this prevents loops and maintains redundancy.

© 2001 Extreme Networks,Inc. All rights reserved

ESRP Switch Behavior

- **Master Switch for the VLAN**
  - Provides L3 functionality for the protected VLAN
  - Performs L2 switching within the VLAN
  - It also exchanges ESRP packets with other standby mode switches
- **Standby Switch for the VLAN**
  - Exchanges ESRP & EDP messages with other switches
  - In L3, marks router interface associated with the VLAN as down
    - This network will not be advertised by the routing protocol
  - In L2, no forwarding occurs between member VLAN ports; preventing loops and maintains redundancy



Notes:

Determining the ESRP "Master"

In The Default Order Of Precedence

The ESRP master switch (the one providing L3 routing and/or layer 2 switching services for a VLAN) is determined by the following factors: These are shown in the default order of precedence. The precedence order is configurable.

- Active ports: The number of active physical links involved with servicing that particular VLAN. The switch that has the greatest number of links takes highest precedence. A load-sharing port group is not considered a single link. If the number of links is equal, the next factor is used.

  Note: Load share ports are not counted as a single port, if four ports are participating; ESRP sees them as four ports. If one of the four fails, a fail over will occur.

  Note: as the number of active ports between a VLAN and the ESRP switches protecting it is often equal (see slide), hence, the 'priority' is often placed first in the order of precedence.

- Tracking: Various types of tracking are used to determine if the switch performing the master ESRP function has connectivity to the outside world. ExtremeWare supports the following types of tracking:

- VLAN – Tracks any active port connectivity to one or more designated VLANs

- IP route table entry – Tracks specific learned routes from the IP route table

- Ping – Tracks ICMP ping connectivity to specified devices.

- Virtual router priority: This is a user-defined field. The range of the priority value is 0 to 255; a higher number has higher priority. The default priority setting is 0. If priorities are equal, the last factor is used.

- Internal MAC address: The higher MAC address has priority

Each switch can be configured using one of five election algorithms to select the ESRP Master, these are:

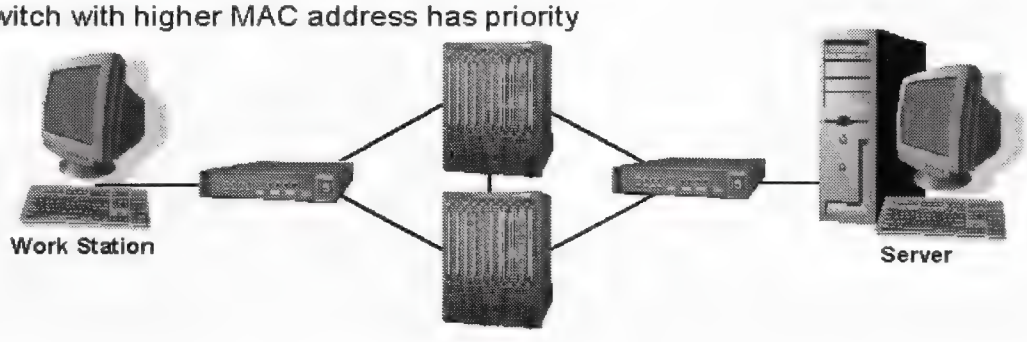
ports_track_priority_mac (default)
Active ports, tracking information, ESRP priority, MAC address
track_ports_priority_mac
Tracking information, active ports, ESRP priority, MAC address
priority_ports_track _mac
ESRP priority, active ports, tracking information, MAC address
priority_track_ports_mac
ESRP priority, tracking information, active ports, MAC address
priority_mac_only
ESRP priority, MAC address

© 2001 Extreme Networks,Inc. All rights reserved

Determining the ESRP "Master"

In The Default Order Of Precedence

- **Active Ports:**
  - Number of active physical links involved in serving the VLAN
  - Switch with greatest number of links takes highest precedence.
- Tracking
  - This is used to track various forms of connectivity from the ESRP switch to the outside world.
- **Priority**
  - The ESRP priority: is set at 0 by default. Configurable from 1 - 255 with higher number taking priority. ***If priority is set to 255, the switch will remain in standby mode even if master fails.***
- **MAC Address**
  - Switch with higher MAC address has priority



Notes:

ESRP Tracking Information Options

Tracking information is used to track various forms of connectivity from the ESRP switch to the outside world. ESRP tracking options are:

ESRP VLAN Tracking

- You can configure ESRP to track connectivity to one or more specified VLANs as criteria for fail-over. If no active ports remain on the specified VLANs, the switch automatically relinquishes master status and remains in standby mode.

ESRP PING Tracking

- You can configure ESRP to track connectivity using a simple ping to any outside responder. The responder may represent the default route of the switch, or any device meaningful to network connectivity of the master ESRP switch. The switch automatically relinquishes master status and remains in standby mode if a ping keep-alive fails three consecutive times.

ESRP Route Table Tracking

- You can configure ESRP to track specified IP routes in the route table as criteria for fail-over. If any of the configured IP routes are not available within the route table, the switch automatically relinquishes master status and remains in standby mode.

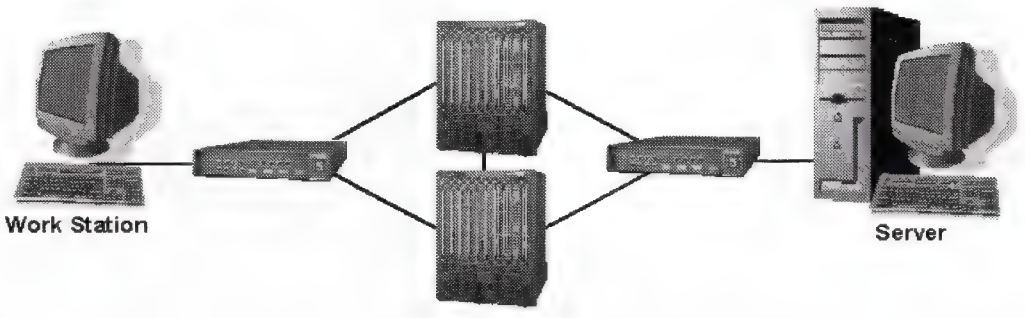
Diagnostic & Health check Tracking

- ESRP is now capable of tracking hardware status. If a power supply or fan fails, or if the chassis is overheating, the priority for the ESRP VLAN will change to the fail-over settings. ESRP will also track the diagnostics that run on each blade. If the diagnostics fail the ESRP VLAN will change the priority to the fail-over settings.

© 2001 Extreme Networks,Inc. All rights reserved

ESRP Tracking Information Options

- **VLAN Tracking**
  - Tracks active port connectivity to one or more specified VLANs
- **Ping Tracking**
  - Tracks ICMP ping connectivity to specified devices.
- **IP Route Table Tracking**
  - Tracks specified learned routes from the IP route table
- **Diagnostics Tracking & Health Checking Tracking**
  - Lost PSU, Fan Failure and over temperature will cause fail over.



Notes:

Example Tracking Configuration

When ESRP tracking is enabled the VLAN will only become the master if the tracking criteria are met.

When the ESRP tracking criteria are not met the ESRP priority of the switch is set to 255. This will put the switch in to Standby.

- The environmental and diagnostic tracking options are exceptions to this rule, as they allow the user to specify the fail over priority

When using ESRP tracking it can be possible to end up in a situation where there are NO masters. Make sure that the tracking criteria can be met without the ESRP protected VLAN being up.

In the example the problem of poor network design is highlighted. Switch 1 has been elected as the ESRP master for VLAN 1 & 2. IP Ping tracking of a device on the Intranet was configured.

If the tracked device fails, or the link from Switch 1 to the Internet/Intranet fails which Switch will becomes the ESRP Master?. What happens to inter VLAN traffic?

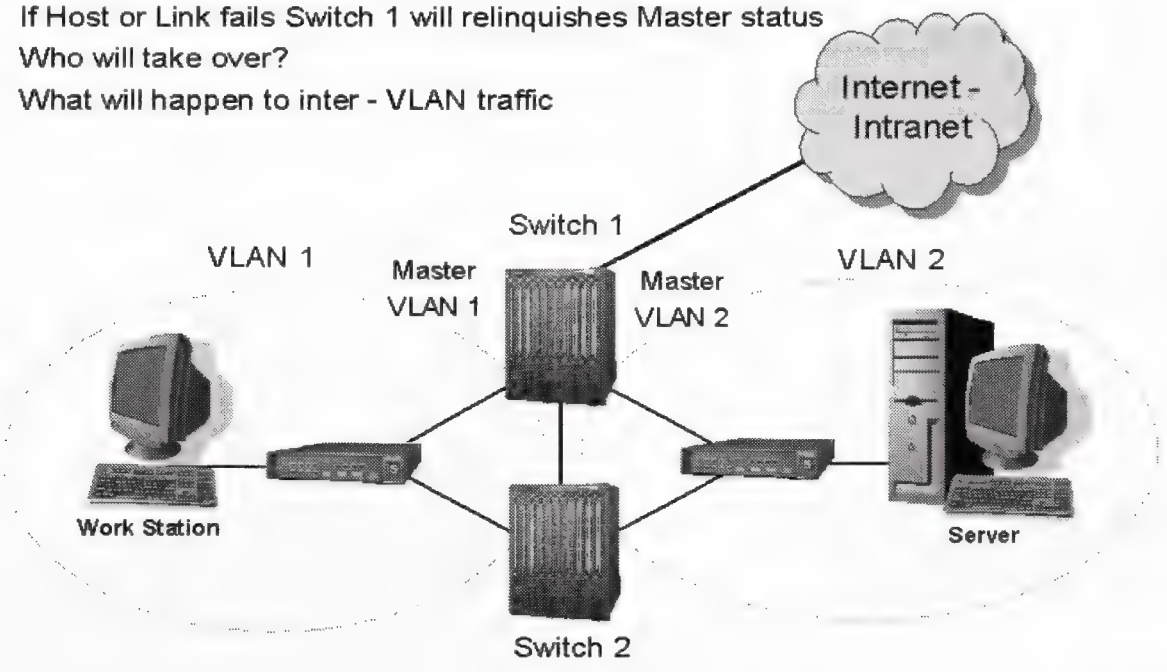
CLI Command - Tracking configuration
config vlan < vlan name> add [track_vlan <vlan name> | track_ping <ipaddress> frequency <seconds> miss <number> | track_iproute <ipaddress> / <netmask> | track_environment failover <priority> | track_diagnostic failover <priority>]

This command allows you to determine the tracking configuration

© 2001 Extreme Networks,Inc. All rights reserved

Example Tracking Configuration

Each Switch is configured with ESRP Ping Tracking of host on Internet/Intranet
If Host or Link fails Switch 1 will relinquishes Master status
Who will take over?
What will happen to inter - VLAN traffic



Notes:

Ways of Electing the Master Switch

A new master can be elected in one of the following ways:

- A communicated parameter change: If a parameter that determines the master changes (for example, number of active ports or priority change), the election of the new master typically occurs within one timer cycle (2 seconds by default).
- Loss of communication between master and slave(s): If there is a communications loss between master and slaves(s), the election of the new master will occur after the slave(s) have missed 3 ESRP hello (6 seconds by default).

Fail-over time is largely determined by the following factors:

- The ESRP timer setting
- The routing protocol being used for inter-router connectivity if Layer 3 redundancy is used. OSPF fail-over time is faster than RIP fail-over time.

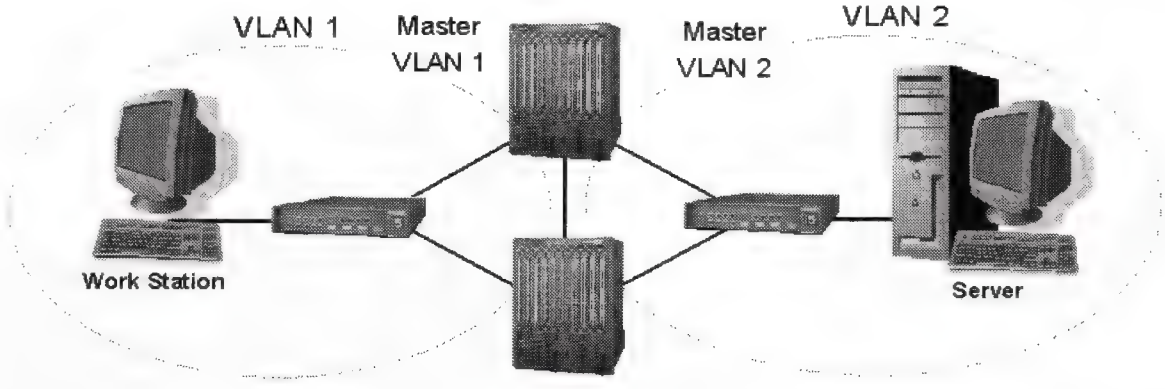
The Fail-over time associated with the ESRP protocol is dependent on the timer setting and the nature of the failure. The default timer setting is 2 seconds; the range is 1 to 255 seconds. Default settings usually result in a Fail-over time of 5 to 8 seconds.

If routing is configured, the Fail-over of the particular routing protocol (such as RIP V1, RIP V2, or OSPF) is added to the Fail-over time associated with ESRP.

© 2001 Extreme Networks,Inc. All rights reserved

Ways of Electing the Master Switch

- **A communicated parameter change**
- **Loss of communication between master and slave/s**
- **Factors in Determining Fail-over Time**
  - The ESRP timer setting
  - The routing protocol being used for inter-router connectivity if Layer 3 redundancy is used



Notes:

ESRP Example

In the slide opposite:
VLAN Client is configured on the Summit 48 switches. This VLAN is ESRP protected by the Summit 7 switches. ESRP is run on the Summit 7 switches, the Summit 48 switches are ESRP aware.

Note the IP address 10.0.0.1 on both switches; this is the User configured IP address of the virtual router. They also use the same Mac address that is pre-configured (discussed later)

The inet VLAN is not ESRP protected (note differing 11.0.0.x IP addresses).

There is no inter-switch link on the Summit 7 switches. This is because the unprotected VLAN (inet) is present on both switches. If the ESRP Master changes, connectivity is maintained.
In the example:

- Both Summit 7 switches have the same number of active ports in the VLAN Client, so either the virtual router priority, tracking or MAC address parameters have determined the Master switch.
- Assuming that the MAC address has determined the Master Switch, what is the effect on Internet/ Intranet traffic if the link between this device and the Intranet/Internet fails?
- All inter VLAN and Internet/Intranet traffic is being switched via one of the Summit 7 switches, the other is in ESRP standby. If further VLANs were configures on these switches we could use the use the priority option to allow the current standby switch to act as the ESRP master for the new VLAN, providing a degree of load sharing.

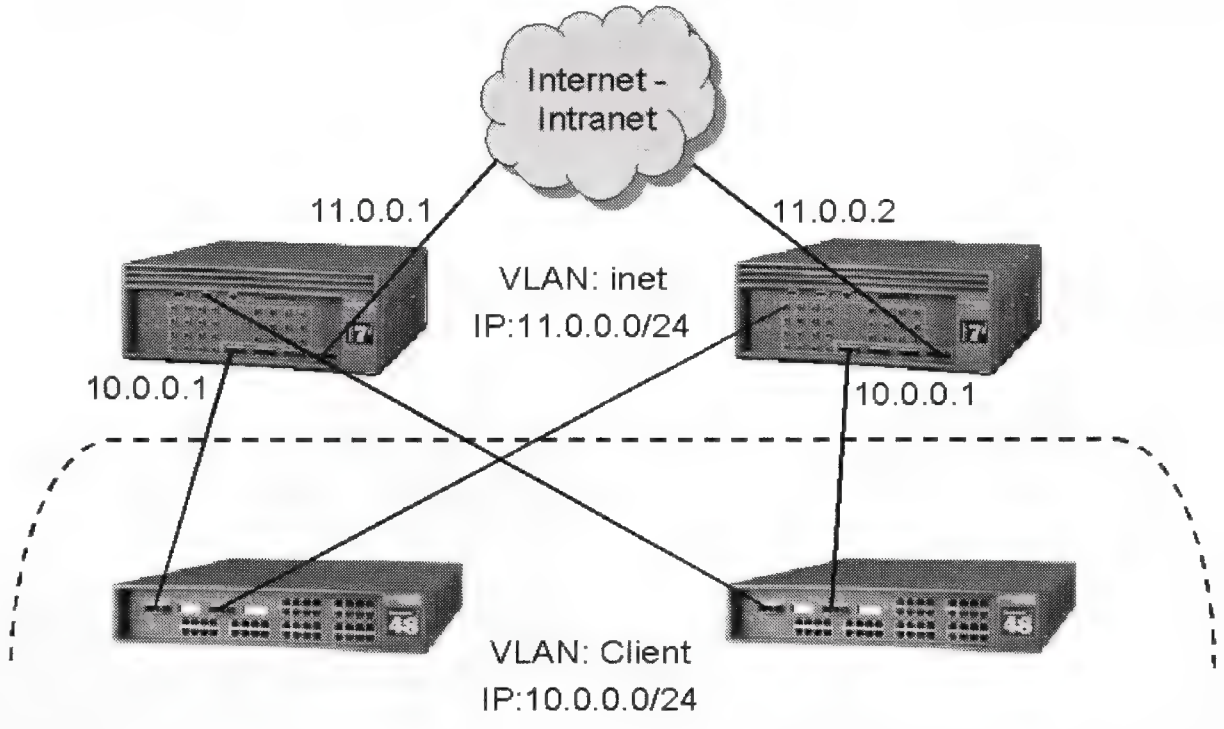
ESRP Configuration information

Left Summit 7i
Configure default del port all
Create vlan client
Create vlan inet
Configure client add port 1,2
Configure inet add port 32
Configure client ipaddress 10.0.0.1/24
Configure inet ipaddress 11.0.0.1/24
Enable ipforwarding
Configure ospf add vlan all area 0.0.0.0
Enable esrp vlan client
Configure ospf routerid 11.0.0.1
Enable ospf

Right Summit 7i
Configure default del port all
Create vlan client
Create vlan inet
Configure client add port 1,2
Configure inet add port 32
Configure client ipaddress 10.0.0.1/24
Configure inet ipaddress 11.0.0.2/24
Enable ipforwarding
Configure ospf add vlan all area 0.0.0.0
Enable esrp vlan client
Configure ospf routerid 11.0.0.2
Enable ospf

© 2001 Extreme Networks,Inc. All rights reserved

ESRP Example



Notes:

Example Display "Show ESRP Detail"

The slide opposite shows the response to the CLI command show esrp detail.

It shows:

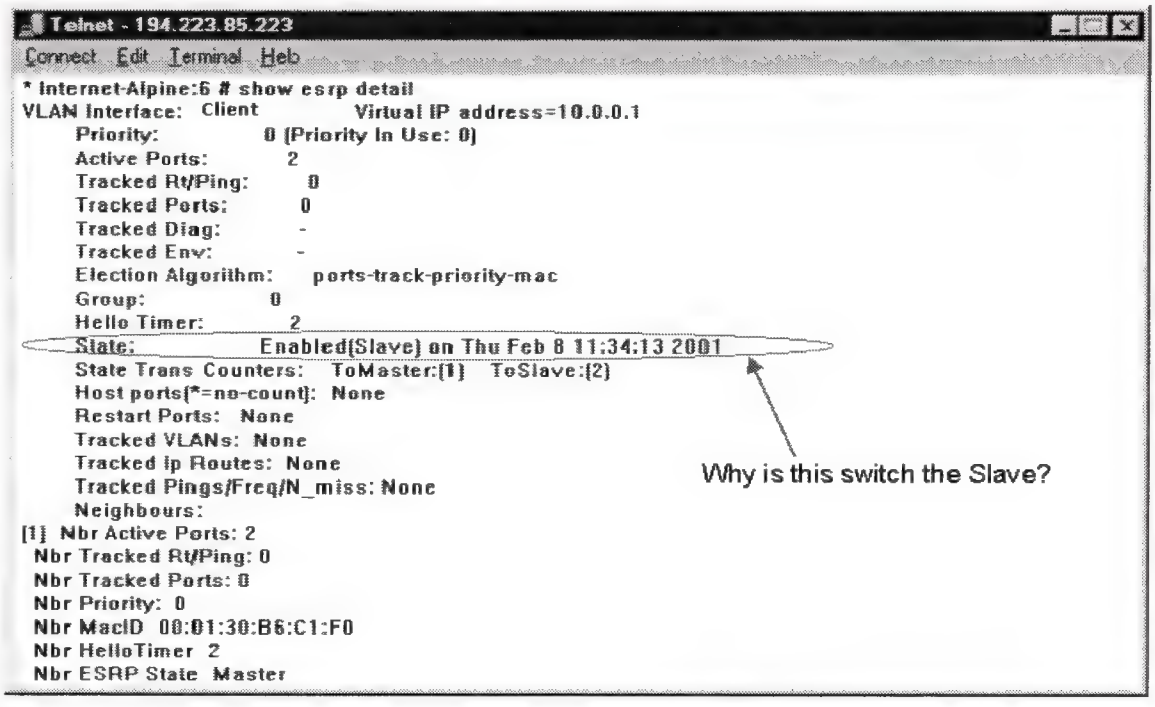
- the VLAN name (Client),
- the Virtual Router address (10.0.0.1)
- Priority of 0
- Active Ports of 2
- Election Algorithm (default)
- The Routers ESRP state – **Slave**.

Further down the trace it shows the Neighbours information. This shows this device as the Master.

From this information can you determine what parameter decided the election of the Master switch and what assumption can you make of the Slave switch?

© 2001 Extreme Networks,Inc. All rights reserved

Example Display "Show ESRP Detail"



Notes:

Steps for Setting up ESRP

- Check the VLAN ports to ensure that EDP is enabled

Extreme Discovery Protocol (EDP) is Extreme Networks proprietary protocol between switches and enabled by default on all ports. EDP must be enabled on the ports that are members of the ESRP VLANs

- Configure the VLANs with the correct ESRP parameters

CLI Command – show port info
show port <portlist> info
Displays port information.

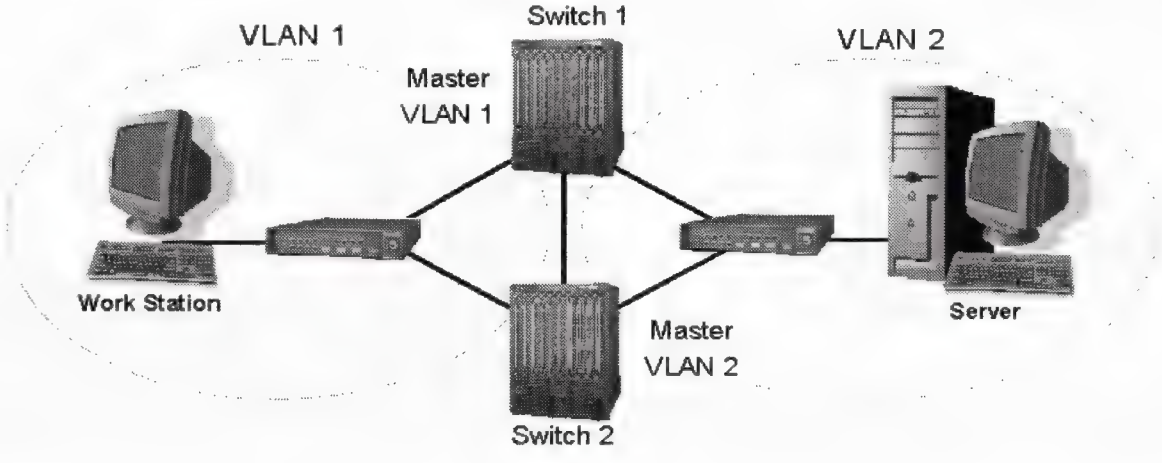
- Enable ESRP

CLI Command – enable ESRP VLAN
enable esrp vlan<vlan name>
Enables ESRP VLAN.

© 2001 Extreme Networks,Inc. All rights reserved

Steps for Setting up ESRP

- **Check to make sure EDP is enabled for all ports in the VLAN with the CLI command:**
  - show port <portlist> info
- **Configure VLAN with correct ESRP parameters**
- **Execute the command:**
  - enable esrp vlan <vlan name>



Notes:

ESRP Options - Host Attach (HA)

ESRP host attach (HA) is an optional ESRP configuration that allows you to connect active hosts directly to an ESRP master or standby switch. Normally, the Layer 2 redundancy and loop prevention capabilities of ESRP do not allow packet forwarding from the standby ESRP switch.

ESRP HA allows configured ports that do not represent loops to the network to continue Layer 2 operation independent of their ESRP status.

The ESRP HA option is useful if you are using dual-homed network interface cards (NICs) for server farms, and in conjunction with high availability server load balancing (SLB) configurations, as shown.

In this example the ESRP Master switch maintains connection to the LAN Cloud. Traffic is forwarded by the master switch to the hosts it connects to, and via the inter-switch link to the slave switch for forwarding on to its directly connected hosts. Traffic is returned from the slave switch via the inter-switch link.

Note: In this case all ports on both switches that are host connected, and the inter-switch link ports, are configured as Host Attached ports.

The ESRP HA feature is used only on switches and I/O modules that have the "i" series chipset.

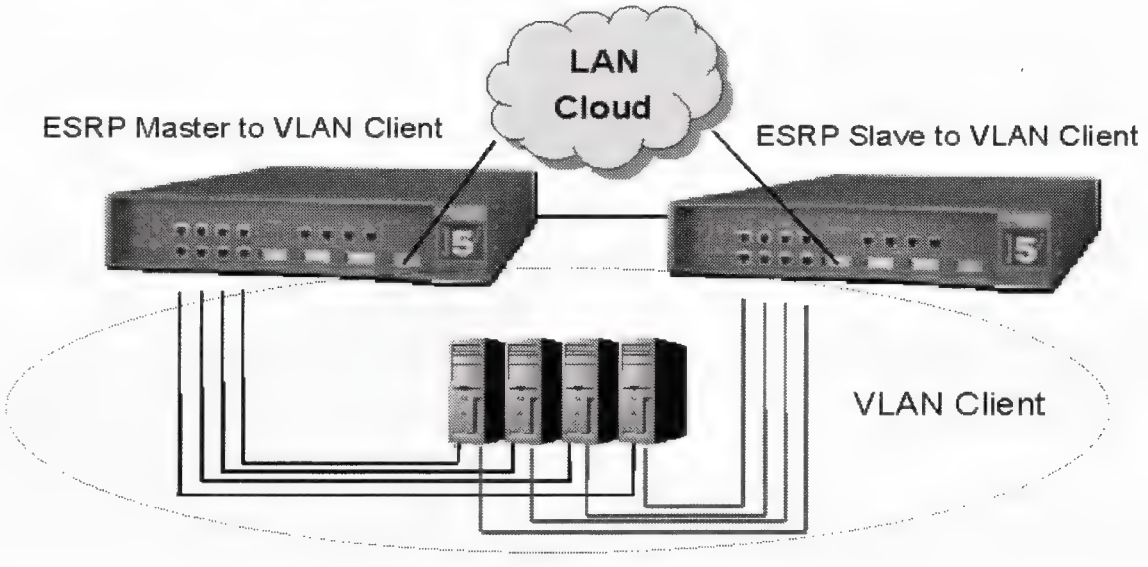
It also requires at least one link between the master and standby ESRP switch for carrying traffic and to exchange ESRP hello packets.

CLI Command – configure port-mode host/normal
configure esrp port-mode [host | normal] ports <port list><cr>
This command enables host attachment

© 2001 Extreme Networks,Inc. All rights reserved

ESRP Options - Host Attach (HA)

- **Allows active hosts to be connected directly to an ESRP Master or standby (slave) switch.**
- **Allows configured ports that do not represent loops, to continue L2 operation independent of ESRP status.**



Notes:

ESRP Options - Domains

ESRP Domains is an optional ESRP configuration that allows you to configure multiple VLANs under the control of a single instance of the ESRP protocol.

By grouping multiple VLANs under one ESRP group, the ESRP protocol can scale to provide protection to large numbers of VLANs.

Note:
All VLANs within an ESRP group simultaneously share the same master and slave switch. In the event of fail-over the master and slave switch will change for ALL domain related VLANs.

The maximum number of ESRP domain member VLANs is 2000.

The CLI command to configure ESRP Domains is:

CLI Command –
configure vlan <vlan name> add domain-member <vlan name><cr>
Add a VLAN to an ESRP domain

The ESRP domain feature is used only on switches and I/O modules that have the "i" series chipset. On the Black Diamond you must first disable support for non "i" chipset products by using the following command:

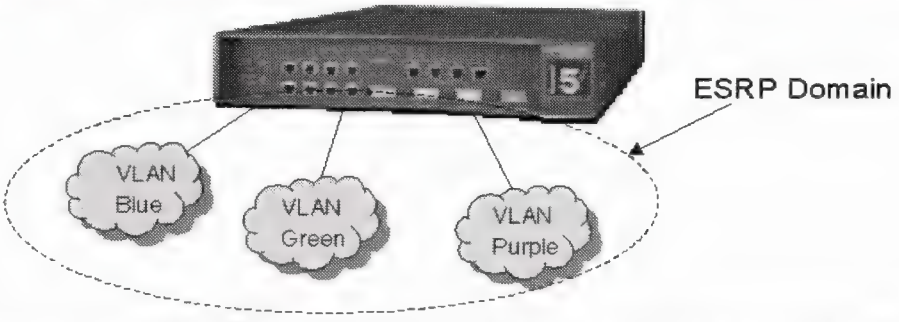
CLI Command –
disable g1-module-support<cr>

You must then set the CPU transmit priority to normal, using the following command:

CLI Command –
configure cpu-transmit-priority normal

© 2001 Extreme Networks,Inc. All rights reserved

ESRP Options - Domains



- The maximum number of ESRP enabled VLANs for a single switch is 64. If you need more VLANs to participate in ESRP you need to configure ESRP domains
- Allows multiple VLANs to be grouped under the control of single instances of the ESRP protocol.
- All VLANs in this particular group share the same Master and Slaves.
- ESRP domain member VLANs max. = 2000

Notes:

Example ESRP Domain

The example shows the configurations for ESRP domains on Summit7i Switches.

Using the command;

CLI Command – show vlan<cr>

will display information on domain members. In this case the display would show:

#show vlan

Name	VID	Protocol Addr	Flags	Proto	Super Ports	
Blue	4093	11.0.0.1/24	E—C-f-----ANY		1/2	C=domain-masterVlan
Purple	4092	10.0.0.1/24	—c-f-----ANY		2/2	c=domain-memberVlan

Using the following command shows the detail for VLAN blue:

CLI command – show vlan blue<cr>

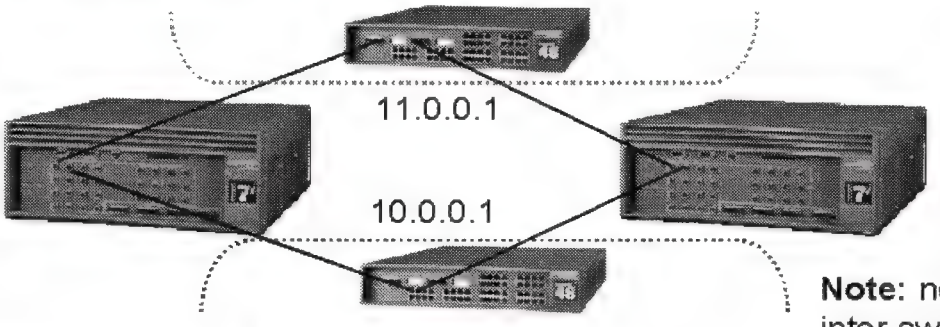
VLAN Interface [3-206] with name "blue" created by user

Tagging:	Untagged (Internal tag 4093)	
IP:	11.0.0.1/255.255.255.0	
STPD:	Domain "s0" is not running spanning tree protocol	
Protocol:	Match all unfiltered protocols	
Loopback:	Disabled	
Rate shape:	Disable	
QosProfile:	QP1	
Ports:	2	(Number of active ports = 2)
Untag:	1 2	

There is no need for an inter-switch link in this example the switch is master for both protected VLANs.

© 2001 Extreme Networks,Inc. All rights reserved

Example ESRP Domain



Note: no need for inter-switch link in this example

Configuration for both Summit7i switches

Summit7i

Configure default del port all
Create vlan blue
Create vlan purple
Configure vlan blue add port 1,2
Configure vlan purple add port 3,4
Configure vlan blue ipaddress 11.0.0.1/24
Configure vlan purple ipaddress 10.0.0.1/24
Enable ipforwarding
Enable esrp vlan blue
Configure vlan blue add domain-member purple

Notes:

ESRP Options - Groups

ExtremeWare supports running multiple instances of ESRP within the same VLAN or broadcast domain. This functionality is called an ESRP group.

Though other uses exist, the most typical application for multiple ESRP groups is when two or more sets of ESRP switches are providing fast-fail-over protection within a subnet.

A maximum of four distinct ESRP groups can be supported within the same-networked broadcast domain.

To configure the ESRP group membership for a VLAN on a switch, use the following command:

CLI Command
config vlan <vlan name> esrp group <group number><cr>

The default group number is 0.
Note: Requires "i" chipset

Every ESRP group uses a different MAC address. These MAC addresses are used as the source of ESRP packets, and as the Layer 3 gateway address.
These addresses are:

Group 0:	00e02b000080
Group 1:	00e02b000081
Group...	.....
Group 31:	00e02b00009F

If you have Host Attached ports that share multiple VLANs, each VLAN must be in a different ESRP group.

- By default all VLANs are put in ESRP group zero (0).

© 2001 Extreme Networks,Inc. All rights reserved

ESRP Options - Groups

- **Allows running multiple instances of ESRP within the same VLAN or broadcast domain**
- **Most typical application for multiple ESRP groups**
  - When two or more sets of ESRP switches are providing fast-failover protection within a subnet
- **Up to four distinct ESRP groups can be supported**
  - Within the same broadcast domain
- **Configure ESRP group membership for a VLAN on a switch with the CLI command:**
  - config vlan <vlan name> esrp group <group number>

*NOTE: **A switch cannot perform both master and slave functions on the same VLAN for separate instances of ESRP***

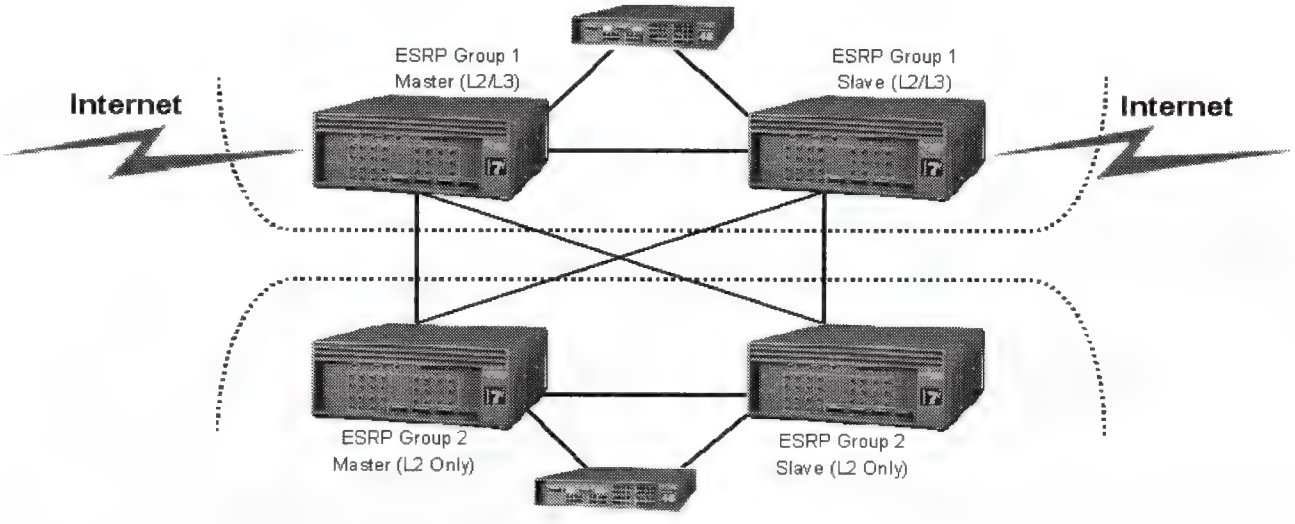
Notes:

ESRP Groups Example

An example ESRP group is shown and discussed on the opposite slide.

© 2001 Extreme Networks,Inc. All rights reserved

ESRP Groups Example



Notes:

ESRP Cautions

When configuring ESRP & Multinetting on a Switch:

- The parameters that affect the determination of the ESRP Master must be configured identically for all VLANs involved with IP multinetting.

Example parameters that must be identical for all affected VLANs are:

- The number of links in your configuration
- The Priority settings
- The Timer settings

When configuring ESRP and Spanning Tree On The Same Switch:

- ESRP and Spanning Tree should not be enabled on the same VLAN/s
- Other switches in the VLAN being protected by ESRP may run STP and the switch running ESRP forwards, but does not filter STP BPDUs.
- Hence, you can combine ESRP and STP on a network and a VLAN, but they must be running on separate devices.
- Care must be taken in maintaining ESRP connectivity between ESRP master and standby switches

© 2001 Extreme Networks,Inc. All rights reserved

ESRP Cautions

- **ESRP should not be enabled on a VLAN that is exchanging routes with other non ESRP routers that use routing protocols like OSPF or RIP.**
  - ESRP could interfere with normal routing communication if an ESRP enabled VLAN contains other routers not using ESRP
- **ESRP and Multi-netting:**
  - When ESRP and IP Multi-netting are on the same switch, the ESRP switches must be configured Identically; ie. Number of links, priority settings, timers, etc.
- **ESRP and Spanning Tree:**
  - Cannot be combined on the same switch.
    - Spanning Tree and ESRP will not work together on the same switch within the same VLAN

Notes:

ESRP and VLAN Aggregation

ESRP can be used to provide redundant default router protection to VLAN aggregation clients.

ESRP is enabled only on the super-VLAN (not the sub-VLANs)

You need to add ports to the super-VLAN that is shared with the sub-VLANs. In order to do this

- Configure the super-VLAN with an 802.1Q tag
- Configure the super-VLANs ports as tagged to avoid protocol conflict.
- Enable ESRP on the super-VLAN

© 2001 Extreme Networks,Inc. All rights reserved

ESRP and VLAN Aggregation

- **ESRP can be used to provide redundant default router protection to VLAN aggregation clients.**
- **ESRP is enabled only on the super-VLAN (not the sub-VLANs)**
- **You need to add ports to the super-VLAN that is shared with the sub-VLANs. In order to do this**
  - Configure the super-VLAN with an 802.1Q tag
  - Configure the super-VLANs ports as tagged to avoid protocol conflict.
  - Enable ESRP on the super-VLAN

Notes:

ESRP: Things to Remember

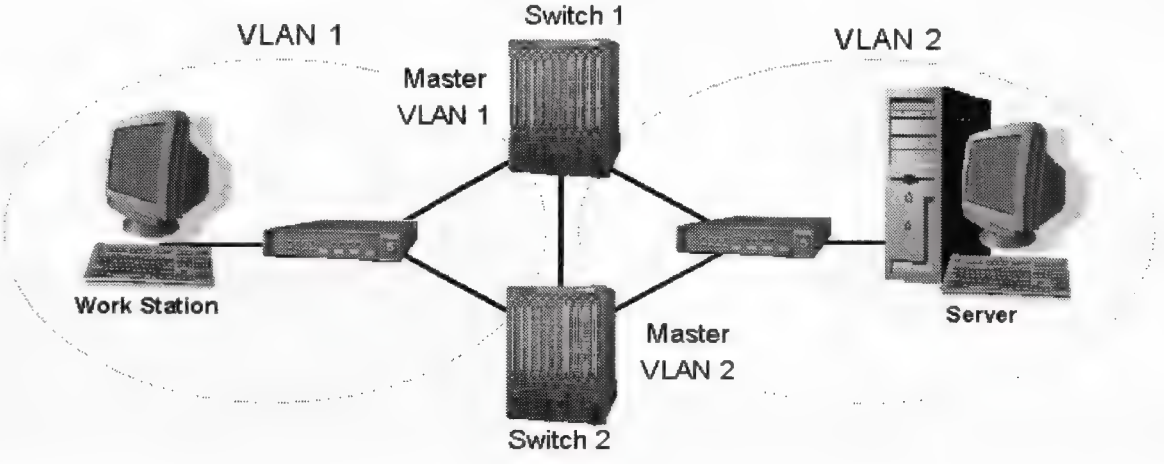
EDP (Extreme Discovery Protocol) must be enabled in order for ESRP to work.

Highly Recommend: Devices must connect to all ESRP routers in the same group, i.e. if there are three ESRP routers, each device must connect to all three ESRP routers.

© 2001 Extreme Networks,Inc. All rights reserved

ESRP: Things to Remember

- **EDP (Extreme Discovery Protocol) must be enabled in order for ESRP to work.**
- ***Highly Recommend*: Devices must connect to all ESRP routers in the same group,**
  - i.e. if there are three ESRP routers, each device must connect to all three ESRP routers.



Notes:

ESRP Commands

CLI command - enable esrp
enable esrp vlan <vlan name><cr>
Enables ESRP on a named VLAN

CLI Command – disable esrp
disable esrp vlan <vlan name> <cr>
Disables ESRP on a named VLAN

CLI Command - config vlan <vlan name> esrp priority <number>
config vlan <vlan name> esrp priority <number><cr>
Configures the ESRP priority. The range is 0 to 255. The higher number has higher priority. The default setting is 0.

CLI Command - config vlan <vlan name> esrp timer <seconds>
config vlan <vlan name> esrp timer <seconds><cr>
Configures the time between ESRP updates. The range is 1 to 255 seconds. The default setting is 2 seconds. The timer setting must be configured identically for the VLAN across all participating switches.

Addition CLI commands relevant to ESRP include:

CLI Command - show esrp detail
show esrp [detail vlan<vlan name> | <all>]<cr>
Displays the ESRP details for a named or all VLANs

CLI Command – enable esrp vlan
enable esrp vlan<vlan name><cr>
Enables ESRP on a named VLAN

CLI Command – disable esrp vlan
disabled esrp vlan<vlan name><cr>
Disables ESRP on a named VLAN

© 2001 Extreme Networks,Inc. All rights reserved

ESRP Commands

CLI command – enable esrp

CLI command – disable esrp

CLI command – config vlan<vlan name>esrp priority<number>

CLI command – config vlan<vlan name>esrp timer<seconds>

CLI command – show esrp detail

CLI command – enable esrp vlan

CLI command – disable esrp vlan

Notes:

Grouping Blocks of 10/100 Ports

Restrictions on port groupings apply only to switches that do not use the "i" chipset.

If you enable ESRP on a VLAN that contains 10/100 ports, a specific block of neighbouring ports must also be participating in a VLAN running ESRP, or must not be used.

The blocks of ports are physically adjacent, regardless of the switch module. For example, the blocks on a BlackDiamond F32T module consist of the following:

- Ports 1-4 and 17-20
- Ports 5-8 and 21-24
- Ports 9-12 and 25-28
- Ports 13-16 and 29-32

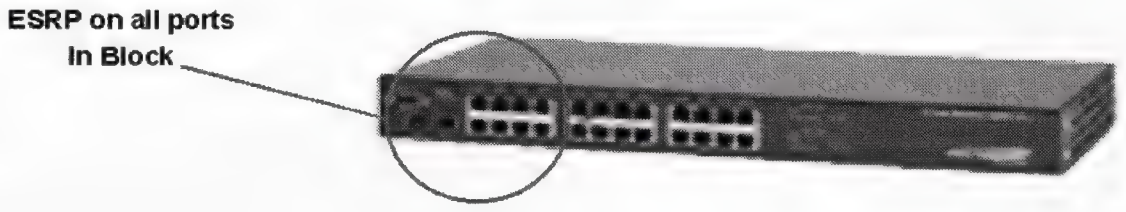
Refer to pages 10-7 and 10-9 in the 6.1 Software User Guide for further information.

© 2001 Extreme Networks,Inc. All rights reserved

Grouping Blocks of 10/100 Ports

Summit non-*i*-based Restriction

- If you enable ESRP on a VLAN that contains 10/100 ports, a specific block of neighbouring ports must also be participating in a VLAN running ESRP, or must not be used.
- The blocks of ports are *physically* adjacent, regardless of the switch or module port numbering scheme.



Notes:

Summary

You should now be able to:

- Describe ESRP in an overview
- Explain the Basics of ESRP
- Describe the Determination of the ESRP Master
- Describe ESRP Tracking Information Option as a Master determinant
- Define the Master Election Algorithm choices and when election occurs
- Describe how to configure ESRP
- Provide ESRP Example Configurations
- Successfully complete the ESRP Lab exercises

© 2001 Extreme Networks,Inc. All rights reserved

Summary

You should now be able to:

- **Describe ESRP**
- **Discuss the Basics of ESRP and define EDP**
- **Describe the Determination of ESRP Master**
- **Discuss ESRP Tracking Information Define the Master Election Algorithm choices and when election occurs**
- **Describe how to configure ESRP**
- **Provide ESRP Example Configurations**
- **Perform the ESRP Lab Exercises**

Notes:

© 2001 Extreme Networks,Inc. All rights reserved

Chapter 12

Introduction to QoS

Chapter Objectives

The main theme of chapter twelve is to discuss the Quality of Service (QoS) options available on the Extreme Networks range of switches.

Upon completion of this chapter, you will be able to:

- Define Policy-Based Quality of Service (QoS)
- Explain types of applications and their QoS requirements
- Define QoS building blocks
- Understand QoS profiles
- Explain traffic groupings and access lists
- Define QoS policy
- Explain the QoS CLI configuration commands
- Define the steps in assigning QoS attributes
- Explain QoS policy modification and verification
- Successfully complete the lab exercises – optional

© 2001 Extreme Networks,Inc. All rights reserved

Chapter Objectives

Upon completion of this chapter, you will be able to:

- **Define Policy-Based Quality of Service (QoS)**
- **Explain types of applications and their QoS requirements**
- **Define QoS building blocks**
- **Understand QoS profiles**
- **Explain traffic groupings and access lists**
- **Define QoS policy**
- **Explain the QoS CLI configuration commands**
- **Define the steps in assigning QoS attributes**
- **Explain QoS policy modification and verification**
- **Successfully complete the lab exercises – optional**

Notes:

What is QoS?

Quality of Service (QoS) is the ability of a network element (e.g. an application, host or router) to have some level of assurance that its traffic and service requirements can be satisfied. To enable QoS requires the cooperation of all network layers from top to bottom, as well as every network element from end to end. Any QoS assurances are only as good as the weakest link in the "chain" between sender and receiver.

QoS does not create bandwidth. It isn't possible for the network to give what it doesn't have, so bandwidth availability is a starting point. QoS only manages bandwidth according to application demands and network management settings, and in that regard it cannot provide certainty if it involves sharing.

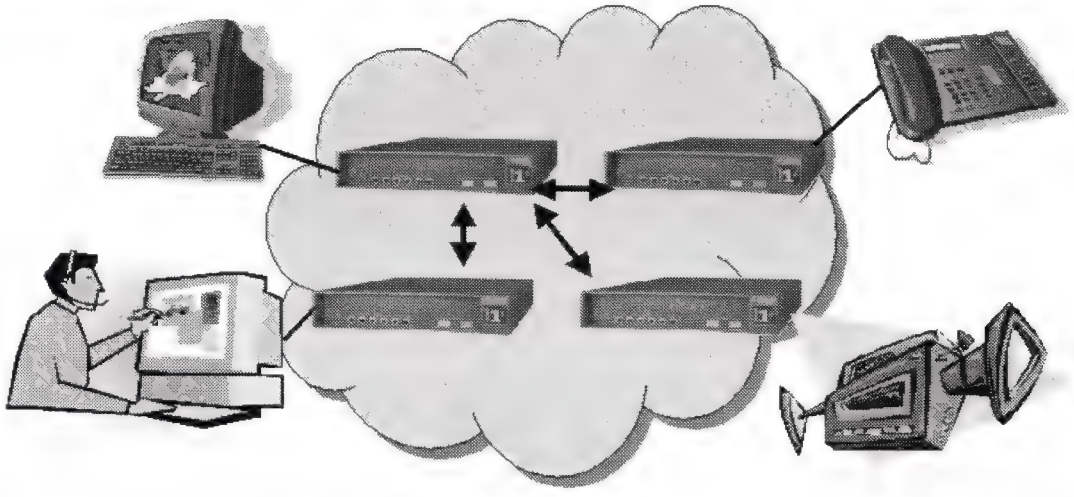
QoS in the Ethernet networks is fundamentally creating unequal access in an essentially equal access network.

Setting the right expectations about QoS:

- A lot of people think that they can control what is inbound. QoS in Extreme Networks switches does not do anything with the inbound traffic (you cannot say 'I want 25% for all 4 types of incoming traffic' and use QoS) - the switch can only apply QoS after traffic has been received and can effect QoS policy going OUTBOUND (destination).
- QoS is not the same as Class of Service (CoS). When CoS assigns a priority to a traffic flow (such as 802.1p) the network elements involved in transporting this information just know that it is more, or less, important than another CoS traffic flow. It does not provide any **assurance** that the information will be provided with a guaranteed bandwidth or network service.

© 2001 Extreme Networks,Inc. All rights reserved

What is QoS?



- Quality of Service (QoS) is to the ability of a network element (e.g. an application, host or router) to have some level of assurance that its traffic and service requirements can be satisfied
- Consists of those mechanisms and protocols designed to facilitate the delivery of delay and bandwidth sensitive material (data/applications) across computer networks.
- *In an Ethernet Network, QoS is used to create unequal access in an essentially equal-access network.*

Notes:

Policy-Based QoS Defined

The main benefit of QoS is that it allows you to have control over the types of traffic that receive enhanced service from the system.

For example:

- If video traffic requires a higher priority than data traffic, using QoS you can assign a different QoS profile to those VLANs that are transmitting video traffic. This profile will assign the video traffic more than a simple high priority, it will provide it with a service level from the underlying network• The agreed profile or service level will provide the traffic with additional characteristics such as maximum or minimum bandwidth guarantees

Voice Applications

Voice applications typically demand small amounts of bandwidth. However, the bandwidth must be constant and predictable because voice applications are typically sensitive to latency (inter-packet delay) and jitter (variation in inter-packet delay). The most important QoS parameter to establish for voice applications is minimum bandwidth, followed by priority.

Video Applications

Video applications are similar in needs to voice applications, with the exception that bandwidth requirements are somewhat larger, depending on the encoding. Key QoS parameters for video applications include minimum bandwidth, priority, and possibly buffering (depending upon the behaviour of the application).

Web Browsing Applications

QoS needs for Web browsing applications cannot be generalised into a single category. For example, ERP applications that use a browser front-end may be more important than retrieving daily news information. The relevant parameter for protecting browser applications is minimum bandwidth. The relevant parameter for preventing non-critical browser applications from overwhelming the network is maximum bandwidth.

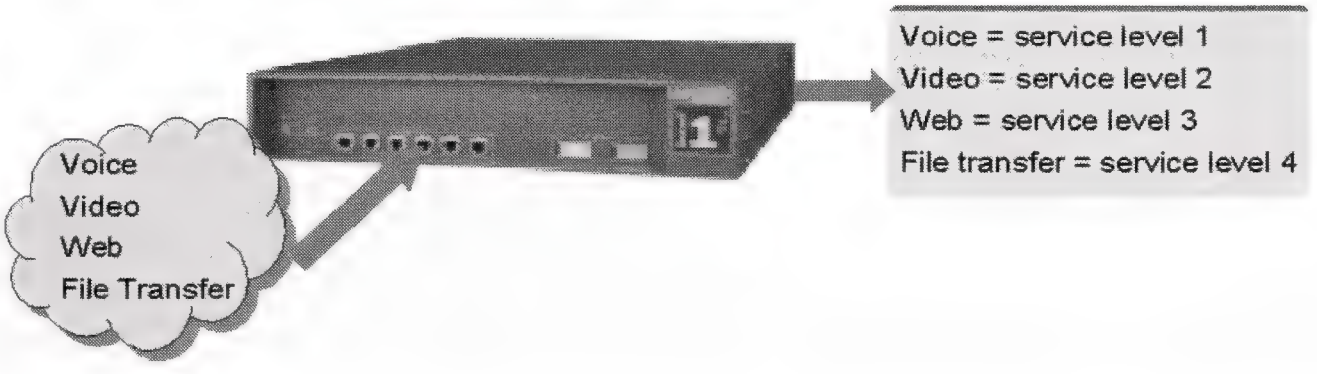
File Server Applications

With some dependencies on the network operating system, file serving typically poses the greatest demand on bandwidth, although file server applications are very tolerant of latency, jitter, and some packet loss, depending on the network operating system and the use of TCP or UDP.

© 2001 Extreme Networks,Inc. All rights reserved

Policy-Based QoS Defined

- **A feature of ExtremeWare and Extreme Networks switch architecture**
  - Allows you to specify different service levels for traffic traversing the switch
  - Allows protection of bandwidth for important categories of applications
  - Or specifically limit bandwidth for less critical traffic
- **An effective control mechanism for networks that have heterogeneous traffic patterns**
- **With QoS, one can specify the service that a traffic type receives**



Notes:

Policy-Based QoS

As with all Extreme Networks Switch products, Policy-Based QoS has zero impact on switch performance. Using even the most complex traffic groupings is "costless" in terms of switch performance.

The switch tracks and enforces the minimum and maximum percentage of bandwidth utilisation transmitted on every hardware queue for every port.

When two or more hardware queues on the same physical port are contending for transmission, the switch prioritises bandwidth use so long as their respective bandwidth management parameters are satisfied.

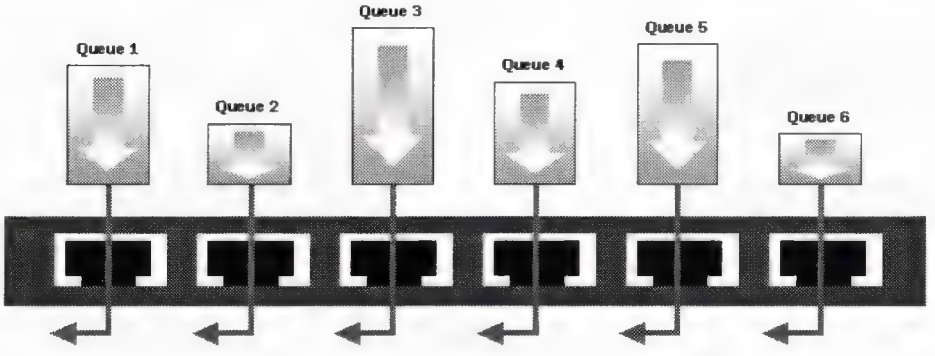
Switch products with the "i" chipset can be configured with up to eight physical queues per port, while other Extreme Networks switches can be configured with up to four physical queues per port.

© 2001 Extreme Networks,Inc. All rights reserved

Policy-Based QoS

- **Contains separate hardware queues on every physical port.**
  - Each queue is programmed by ExtremeWare with
    - Bandwidth Management, and
    - Prioritisation Parameters

- **Tracks and enforces MIN and MAX percentages of the total link bandwidth that is reserved for use by a hardware queue on a physical port**



Notes:

When do you need QoS?

QoS is required when differing network traffic needs a guarantee of underlying network performance. This typically relates to the amount of bandwidth required, but other factors, such as priority, are also taken into account.

Historically, bandwidth (or the lack of it) was mainly a concern of Wide Area Network technologies as Local Area Network technologies were developing at such a pace and were delivering bandwidths of 10, 100 and 1000Mbps. In the LAN we were able to over-provision the available bandwidth to ensure that all network traffic receives an adequate service.

The rapid development and deployment of applications within the marketplace has placed an increasing strain on LAN infrastructures. The increasing requirement for greater performance from both the underlying transport technologies and the physical network hardware has resulted in the development of the products we are familiar with today. Products and technologies such as Layer 2 switches, Layer 3 switches, ASICs and multi-layer switches have all resulted from this quest for greater network performance.

The availability of high performance LAN technologies and hardware means that some organisations can provide the levels of service required by their applications by simply over-provisioning their LAN infrastructure. This provides a simple, but not managed, solution to their requirements.

"Throwing bandwidth" at the issue of application performance does provide a simple solution, but it does not resolve the underlying issue of supporting the ever-increasing demands of new applications (voice, web, video, etc.) in an efficient and controlled manner.

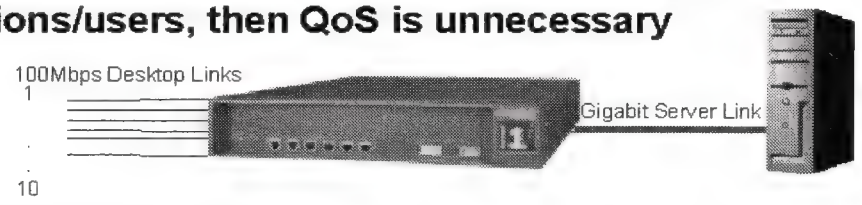
The differing requirements of the mixture of application traffic found on modern networks can only be supported in a managed fashion by developing QoS networks. In this environment, an application is assured that its requirement for bandwidth, priority, latency and delay can be provided for.

Remember:
QoS does not increase the available bandwidth; it ensures that it is used in a controlled manner. The network designer still has to make sure that the network has sufficient capacity and throughput to deliver the service required.

© 2001 Extreme Networks,Inc. All rights reserved

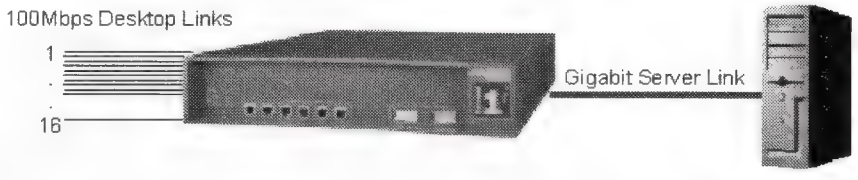
When do you need QoS?

- **If a network provides enough bandwidth for all applications/users, then QoS is unnecessary**



Not Oversubscribed Configuration ⟷ **No QoS Required**

- **If there is insufficient bandwidth...**
  - ...and the network has an oversubscribed configuration, then QoS can provide prioritised service for those applications that are sensitive to the resultant latencies or delays.



Oversubscribed Configuration ⟷ **QoS Might Make Sense**

Notes:

When is QoS Required? - Latency Control

In the early days of LAN technology the majority of traffic required a reliable, error free environment rather than guaranteed throughput. The CSMA/CD access method of Ethernet supports this.

This was because the traffic was primarily batch oriented. While there has always been the requirement for a 'quick' network, the measurement for this speed was often how long a user was prepared to wait for a response once a request was issued. As long as the network provide a 'fast' enough response, it was suitable.

In the modern environment requirements have changed.

The network is now a vital section of the company's infrastructure. It carries information that is critical to the operation and success of the organisation. The network has to balance the needs of multiple applications, many of which were not envisaged when the underlying technology was developed.

Modern LAN infrastructures carry traffic that was originally designed to run over several different technologies, each with their own characteristics. The modern network has to provide each of these applications with the characteristics it requires, which may not have been part of it's own original design.

Unlike the original characteristics of 'error free with non-deterministic access' provided by Ethernet, many of these newer applications are time sensitive, and the overall latency of the network is important.

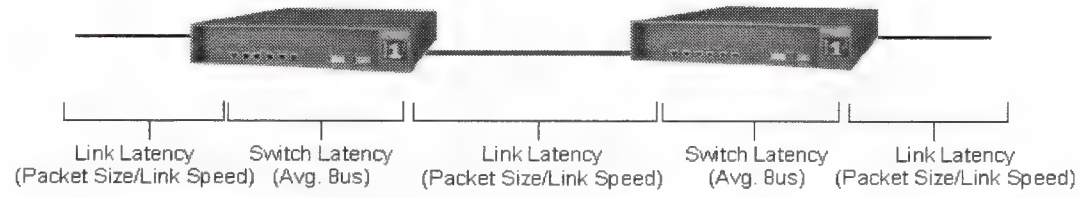
QoS can provide controls over minimum and maximum bandwidth availability to ensure that latency parameters are met.

© 2001 Extreme Networks,Inc. All rights reserved

When is QoS Required? - Latency Control

- **Provide consistent end-to-end delay to flows**

- **Delay-sensitive applications**
  - Desktop Video Conferencing
  - Multicast Streaming Video
  - Real-Time Data Feeds (e.g., Financial Applications)
  - SNA, TN3270



- **The most important QoS parameter for delay sensitive applications is minimum bandwidth, followed by priority**

Notes:

When is QoS Required? - Congestion Management

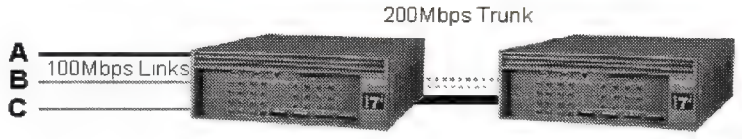
Another feature of QoS is its ability to 'share' the available bandwidth between different types of traffic. This is typically by allocating a maximum or minimum percentage of the available bandwidth to a specified class of traffic. The example highlights this ability.

QoS can only share what is available; the network designer has to ensure that the overall bandwidth is adequate.

© 2001 Extreme Networks,Inc. All rights reserved

When is QoS Required? - Congestion Management

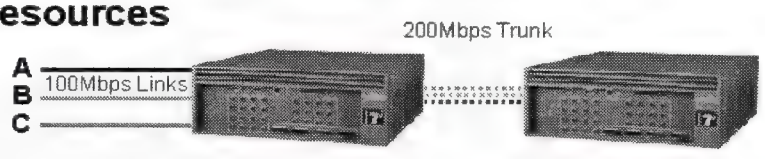
- **Important traffic bypasses congestion**



Option 1
Traffic Group A gets QP2
Other Traffic Groups get QP1

Option 2
Traffic Group A gets MinBW=50%
Other Traffic Groups get MinBW=25%

- **Multiple Traffic Groups are allowed equal access to congested resources**



Option 1
All Traffic Groups get MinBW=33%

Notes:

Traffic Type and QoS Guidelines

Different applications have different QoS requirements. The following applications are ones that you will most commonly encounter and need to prioritise:

- Voice applications
- Video applications
- Critical database applications
- Web browsing applications
- File server applications

General guidelines for each traffic type are given below and summarised in the opposite table.

Consider them as general guidelines and not strict recommendations. Once QoS parameters are set, you can monitor the performance of the application to determine if the actual behaviour of the applications matches your expectations. It is very important to understand the needs and behaviour of the particular applications you wish to protect or limit. Behavioural aspects to consider include bandwidth needs, sensitivity to latency and jitter, and sensitivity and impact of packet loss.

© 2001 Extreme Networks,Inc. All rights reserved

Traffic Type and QoS Guidelines

Traffic Type	Key QoS Parameters
Voice	Minimum Bandwidth, priority
Video	Minimum Bandwidth, priority, buffering (varies)
Database	Minimum Bandwidth
Web browsing	Minimum Bandwidth for critical applications, maximum bandwidth for non-critical applications
File Server	Minimum Bandwidth

Notes:

The Building Blocks of QoS

Assigning QoS attributes is a three-step process, which consists of defining three interrelated QoS building blocks.

Create a QoS profile.

- QoS profile — A class of service that is defined through minimum and maximum bandwidth parameters, configuration of buffering and prioritisation settings. The bandwidth and level of service that a particular type of traffic or "traffic grouping" receives is determined by assigning it to a QoS profile.

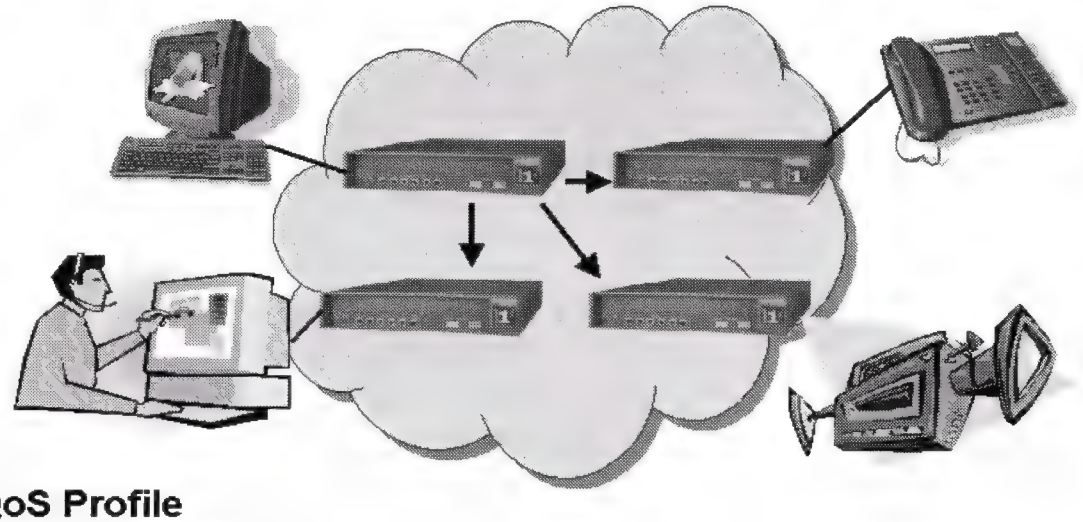
Assign one or more traffic groupings.

- Traffic grouping — A classification or traffic type that has one or more attributes in common. These can range from a physical port to a VLAN to IP Layer 4 port information. Traffic groupings transmitting out of the same port that are assigned to a particular QoS profile share the assigned bandwidth and prioritisation characteristics, and hence share the class of service.
- QoS policy — The combination that results from assigning a traffic grouping to a QoS profile.

Monitor the performance of the application with the QoS monitor to determine whether the policies are getting the desired results.

© 2001 Extreme Networks,Inc. All rights reserved

The Building Blocks of QoS



- QoS Profile
- Traffic Grouping
- QoS Policy
- ***Assigning QoS attributes is a three-step process consisting of defining each of the three building blocks***

Notes:

QoS Building Block

A QoS profile defines a class of service by specifying traffic behaviour attributes, such as bandwidth. The parameters that make up a QoS profile include the following:

- Minimum bandwidth
- Maximum bandwidth
- Priority
- Buffer

A QoS profile does not alter the behaviour of the switch until it is assigned to a traffic grouping. Recall that QoS profiles are linked to hardware queues. There are multiple hardware queues per physical port. By default, a QoS profile links to the identical hardware queue across all the physical ports of the switch.

© 2001 Extreme Networks,Inc. All rights reserved

QoS Building Block

1 - QoS Profile

- **Defines a class of service by specifying traffic behaviour attributes like bandwidth**
- **Does not alter the behaviour of switch until it is assigned to a traffic grouping**
- **By default, a QoS profile links to the identical hardware queue across all switch physical ports**
- **Four or eight default QoS profiles are provided based on the switch chipset**
  - QP1 – QP4 for non-"i" based chipset
  - QP1 - QP8 for "i" series chipset

Notes:

QoS Profile Parameters

Minimum bandwidth

- The minimum percentage of total link bandwidth that is reserved for use by a hardware queue on a physical port. Bandwidth unused by the queue can be used by other queues. The minimum bandwidth for all queues should add up to less than 90%. The default value on all minimum bandwidth parameters is 0%.

Maximum bandwidth

- The maximum percentage of total link bandwidth that may be transmitted by a hardware queue on a physical port. The default value on all maximum bandwidth parameters is 100%.

Priority

- The level of priority assigned to a hardware queue on a physical port.

Switch products that use the "i" chipset have eight different available priority settings. Other Extreme Networks switches have four available priority settings. By default, each of the default QoS profiles is assigned a unique priority. You would use prioritisation when two or more hardware queues on the same physical port are contending for transmission on the same physical port, only after their respective bandwidth management parameters have been satisfied. If two hardware queues on the same physical port have the same priority, a round-robin algorithm is used for transmission, depending on the available link bandwidth.

When configured to do so, the priority of a QoS profile may determine the 802.1p bits used in the priority field of a transmitted packet. On switch products using the "i" chipset, the priority of a QoS profile determines the DiffServ code point value used in an IP packet when the packet is transmitted.

Buffer

- This parameter reserves buffer memory for use exclusively by a QoS profile across all affected ports. The default value for buffer settings is 0%. The sum value of all QoS profile buffer parameters should not exceed 100%. Reserving buffer memory for a QoS profile affects the dynamic buffer space available to other QoS profiles. You should not modify the buffer parameter unless specific situations and application behaviour indicate that you should do so.

© 2001 Extreme Networks,Inc. All rights reserved

QoS Profile Parameters

- **Minimum bandwidth**
  - Minimum % of total link bandwidth reserved for use by a hardware queue on a physical port. Default value is 0%. Bandwidth unused by the queue can be used by other queues. All queues should add up to less than 90%.
  - Minimum bandwidth guarantees are met first
- **Maximum bandwidth**
  - Maximum % of total link bandwidth that may be transmitted by a hardware queue on a physical port. Default value is 100%.
- **Priority**
  - Level of priority assigned to a hardware queue on a physical port.
  - Use prioritisation when two or more hardware queues on the same physical port are contending for transmission on the same physical port only after bandwidth parameters are satisfied.
  - Priority determines which profile receives the rest of the available bandwidth
- **Buffer**
  - Reserves buffer memory for use exclusively by a QoS profile across all affected ports. Default setting is 0%

Notes:

QoS Profile Mapping

Four or eight default QoS profiles are provided, depending on the chipset used in the switch. By default, a QoS profile maps directly to a specific hardware queue across all physical ports.

In the table opposite, the settings for the default QoS profiles for non-i chipset products are summarised, as well as the settings for i-based chipset products.

To create a new QoS profile the following command is used:

CLI Command – create qosprofile
create qosprofile <qosname> <cr>
Creates a QoS profile in EGRESS mode.

The default values assigned to a created QoS profile are:

- Minimum bandwidth = 0%
- Maximum bandwidth = 100%
- Priority – low

Using the following command modifies these values:

CLI Command – config qosprofile
Config qosprofile <qosname> {minbw <percent>}{maxbw <percent>}{priority[high highHi low lowHi medium mediumHi normal normalHi] {maxbuf minbuf <port number>} <cr>

Minibw
The minimum bandwidth percentage guaranteed to be available to this queue. The default setting is 0

Maxbw
The maximum bandwidth percentage guaranteed to be available to this queue. The default setting is 100

Priority
The service priority for this queue. The default setting is low. Available in egress mode only.

Max/min buf
This parameter allows you to set maximum and minimum buffers for each queue, so a single queue will not consume all the unallocated buffer space.

© 2001 Extreme Networks,Inc. All rights reserved

QoS Profile Mapping

Default QoS Profiles for non-"i" Chipset Products					
Profile Name	Hardware Queue	Priority	Buffer	Minimum Bandwidth	Maximum Bandwidth
Qp1	Q0	Low	0	0%	100%
Qp2	Q1	Normal	0	0%	100%
Qp3	Q2	Medium	0	0%	100%
Qp4	Q3	High	0	0%	100%
Default QoS Profiles for "i" Chipset Products					
Qp1	Q0	Low	0	0%	100%
Qp2	Q1	Lowhi	0	0%	100%
Qp3	Q2	Normal	0	0%	100%
Qp4	Q3	Normalhi	0	0%	100%
Qp5	Q4	Medium	0	0%	100%
Qp6	Q5	Mediumhi	0	0%	100%
Qp7	Q6	High	0	0%	100%
Qp8	Q7	Highhi	0	0%	100%

Notes:

QoS Building Block - Traffic Groupings

Once a QoS profile is modified for bandwidth and priority, you assign the profile to a particular traffic grouping. A QoS profile is assigned to a specific traffic grouping to create a QoS policy. A *traffic grouping* is a classification of traffic that has one or more attributes in common.

© 2001 Extreme Networks,Inc. All rights reserved

QoS Building Block

2 – Traffic Groupings

- **A classification or traffic type that has one or more attributes in common**
- **Are assigned to QoS profiles to modify switch forwarding behavior**
- **Those groupings transmitting out of the same port and assigned to a particular QoS profile will:**
  - Share the assigned bandwidth and prioritisation characteristics, hence sharing the class of service

Notes:

Traffic Groupings in Order of Precedence

Once a QoS profile is modified for bandwidth and priority, you assign the profile to a particular traffic grouping in order to create a QoS policy.
Traffic groupings classify traffic having one or more attributes in common.

In the event that a given packet matches two or more grouping criteria, there is a predetermined precedence for which traffic grouping will apply. In general, the more specific traffic grouping takes precedence. By default, all traffic groupings are placed in the QoS profile QP1. ExtremeWare supports the shown listed traffic groupings in the order of precedence (highest to lowest).

IP-based traffic groupings
IP-based traffic groupings are based on any combination of:

- IP source or destination address
- TCP/UDP port information

IP-based traffic groupings are defined using access lists. Access lists are discussed later. This level of packet filtering has no impact on performance.

MAC-based traffic groupings
QoS profiles can be assigned to destination MAC addresses. The MAC address options are as follows:

- Permanent
- Dynamic
- Blackhole
- Broadcast/unknown rate limiting

Explicit packet class of service- based traffic groupings
This category of traffic groupings describes what is sometimes referred to as explicit packet marking, and refers to information contained within a packet intended to explicitly determine a class of service. That information includes:

- IP DiffServ code points, formerly known as IP TOS bits
- Prioritisation bits used in IEEE 802.1p packets

Physical/Logical groupings
Two traffic groupings exist in this category:

- Source port
- VLAN

A source port traffic grouping implies that any traffic sourced from this physical port uses the indicated QoS profile when the traffic is transmitted out to any other port.

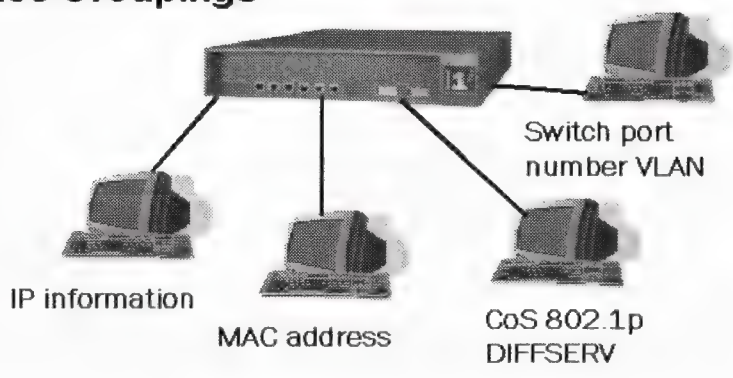
A VLAN traffic grouping indicates that all intra-VLAN switched traffic and all routed traffic sourced from the named VLAN uses the indicated QoS profile

© 2001 Extreme Networks,Inc. All rights reserved

Traffic Groupings

In Order of Precedence

- **IP-based information (Access Lists) Groupings**
  - IP source or destination address
  - TCP/UDP port information
- **Destination MAC address Groupings**
  - Permanent
  - Dynamic
  - Blackhole
  - Broadcast/unknown rate limiting
- **Explicit Packet Class of Service Groupings**
  - DiffServ (IP TOS)
  - 802.1P
- **Physical/Logical Groupings**
  - Source Port
  - VLAN



Notes:

What are Access Lists

Access lists consist of IP access rules, and are used to perform packet filtering and forwarding decisions on incoming traffic. Each packet arriving on an ingress port is compared to the access list in sequential order, and is either forwarded to a specified QoS profile or dropped. Using access lists has no impact on switch performance.

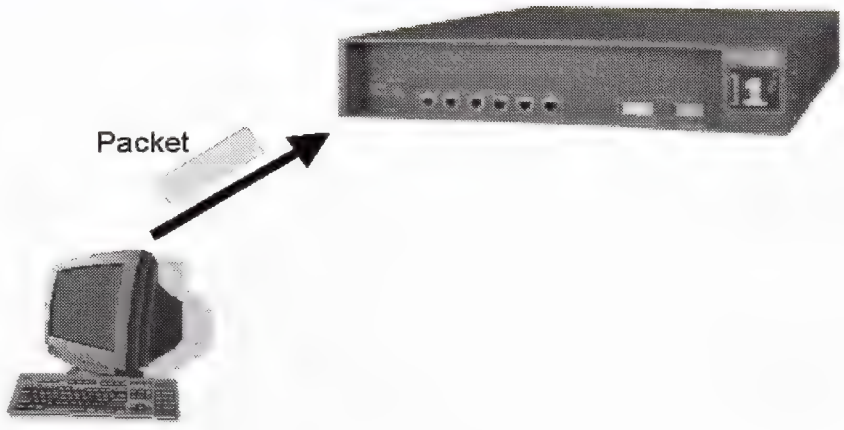
Access lists are typically applied to traffic that crosses layer 3 router boundaries, but it is possible to use access lists within a layer 2 VLAN.

Products that use the "i" chipset are capable of performing this function with no additional configuration. Products that do not use the "i" chipset require the enabling of Intra-subnet QoS (ISQ), to perform this function.

© 2001 Extreme Networks,Inc. All rights reserved

What are Access Lists

- **An IP Access List is a list of IP Access rules, which are used to perform packet filtering and make forwarding decisions for every incoming packet. Depending on the device this can either be done in hardware or software**



Notes:

Traffic Groupings - IP Based

As mentioned earlier, IP-based traffic groupings are defined using Access Lists based on any combination of:

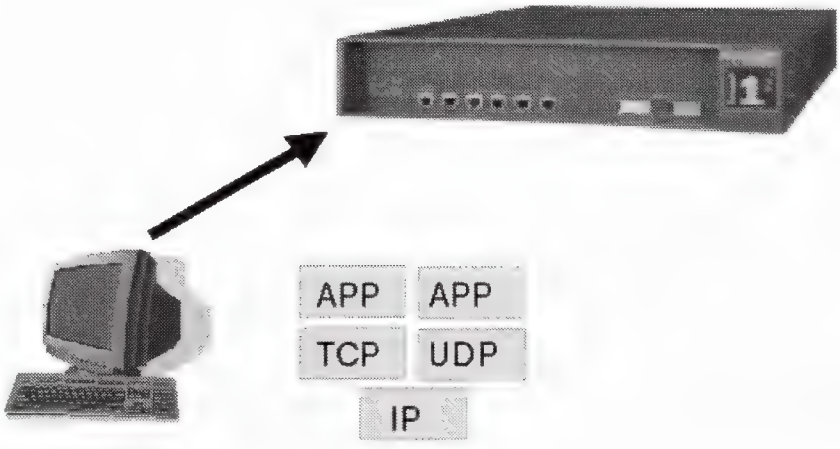
- IP source or destination address
- TCP/UDP port information

It is important to realise that an IP-based traffic group my only specify a TCP or UDP port number. The inclusion of IP addressing information is not mandatory. The following slides provide greater detail on IP Access Lists.

© 2001 Extreme Networks,Inc. All rights reserved

Traffic Groupings

IP-Based



- **Defined using Access Lists**
- **A packet that matches the access list will be forwarded using the configured QoS profile**
- **This level of packet filtering has no impact on performance**

Notes:

Extreme Access Lists - 1

How Access Lists Work

When a packet arrives on an ingress port, the packet is compared with the access list rules to determine a match. When a match is found, the packet is processed. If the access list is of type deny, the packet is dropped. If the list is of type permit, the packet is forwarded. A permit access list can also apply a QoS profile to the packet.

Each entry that makes up an IP access list contains a unique name. It can also contain an optional, unique precedence number. The rules of an IP access list consist of a combination of the following six components:

- IP source address range
- IP destination address range
- TCP or UDP source port range
- TCP or UDP destination port range

Specifying a Default Rule

To begin constructing an access list, you should specify a default rule. A default rule is a rule that contains wildcards for destination and source IP address, with no Layer 4 information. A default rule determines if the behaviour of the access list is an "implicit deny" or "implicit accept". If no access list entry is satisfied, the default rule is used to determine whether the packet is forwarded or dropped. If no default rule is specified, the default implicit behaviour is to forward the packet.

© 2001 Extreme Networks,Inc. All rights reserved

Extreme Access Lists 1

- **How does it work?**
  - When a packet arrives on an ingress port, the packet is compared with the access list rules in sequential order to determine a match. When a match is found, the packet is processed. If the access list is of type deny, the packet is dropped. If the list is of type permit, the packet is forwarded. A permit access list can also apply a QoS profile to the packet.

- **What type of IP Access Lists do we have?**
  - IP access list
  - UDP access list
  - TCP access list
  - ICMP access list

- **Except for the ICMP access list, all processing is done in *hardware.***

Notes:

Extreme Access Lists 2

Precedence Number

The precedence number is optional, and determines the order in which each rule is examined by the switch. Access list entries that contain a precedence number are evaluated from highest to lowest. Precedence numbers range from 1 to 25,600, with the number 1 having the highest precedence.

You can specify overlapping rules, however, if you are using precedence numbers, overlapping rules without precedence numbers are ignored. Therefore, the precedence numbers must be specified among all overlapping rules. If a new rule without a precedence number is entered, and this rule overlaps with already existing rules, the switch rejects the new rule and resolves the precedence's among all remaining overlapping rules.

Maximum Entries

A maximum of 255 entries with an assigned precedence can be used. In addition to the 255 entries, entries that do not use precedence can also be created, with the following restrictions:

- A source IP address must use wildcards or be completely specified (32 bit mask)
- The layer 4 source and destination ports must use wildcards or be completely specified (no ranges)
- No physical source port can be specified
- Access list rules that apply to all physical ports are implemented on all BlackDiamond I/O modules

On a BlackDiamond 6808 switch the maximum number of access list entries is 255 entries per I/O module. One way to economise on the number of entries on a BlackDiamond switch is to provide a physical ingress port as a component of an access list rule. In this case, the rule is implemented only on the I/O modules that contain the specified ports. By restricting rules to specific I/O modules, you can extend the number of access list rules to 2,040 (255 * 8).

© 2001 Extreme Networks,Inc. All rights reserved

Extreme Access Lists 2

- **Precedence number:**
  - The precedence number is optional, and determines the order in which each rule is examined by the switch. Precedence numbers range from 1 to 25,600, with the number 1 having the highest precedence.
  - *Advice*: **ALWAYS** use a precedence number, as rules without one can be put anywhere in the list!! Also other side effects might occur (see later in the presentation).

- **Maximum ACL entries:**
  - Maximum of 255 ACL entries are supported per switch, or 255 per I/O module when you are using a BlackDiamond chassis. In addition a total of 1024 *flow ACLs* are supported.

Notes:

Traffic groupings - Destination MAC Adress

QoS profiles can be assigned to destination MAC addresses. MAC-based traffic groupings are configured using the following command:

CLI Command - create fdbentry

create fdbentry <mac_address> vlan <name> [blackhole | port <portlist> | dynamic] qosprofile <qosprofile>

The MAC address options are as follows:

- Permanent
- Dynamic
- Blackhole
- Broadcast/unknown rate limiting

Permanent MAC addresses

Permanent MAC addresses can be assigned a QoS profile whenever traffic is destined to the MAC address.

Dynamic MAC Address

Dynamic MAC addresses can be assigned a QoS profile whenever traffic is destined to the MAC address. For any port on which the specified MAC address is learned in the specified VLAN, the port is assigned the specified QoS profile. The QoS profile is assigned when the MAC address is learned. If a client's location moves, the assigned QoS profile moves with the device. If the MAC address entry already exists in the FDB, you can clear the forwarding database so that the QoS profile can be applied when the entry is added again.

Blackhole MAC Address

Using the blackhole option configures the switch to not forward any packets to the destination MAC address on any ports for the VLAN specified.

Broadcast/Unknown Rate Limiting MAC Address

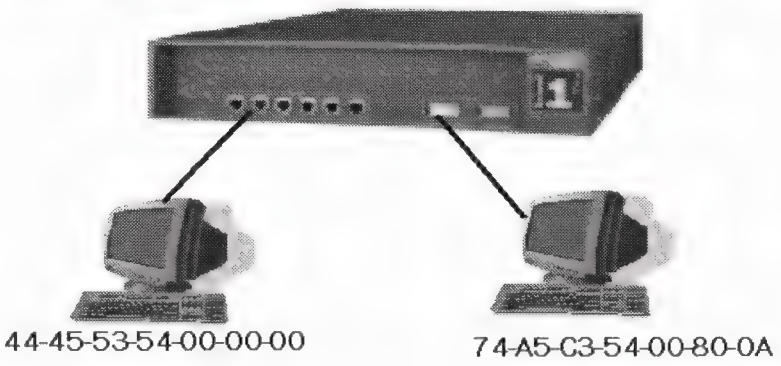
It is possible to assign broadcast and unknown destination packets to a QoS profile that has the desired priority and bandwidth parameters. Broadcast/unknown rate limiting is an extension of the QoS feature used for destination MAC addresses.

IP multicast traffic is subject to broadcast and unknown rate limiting only when IGMP snooping is disabled.

© 2001 Extreme Networks,Inc. All rights reserved

Traffic Groupings

Destination MAC Address



- **The MAC Address options are:**
  - Permanent
  - Dynamic
  - Blackhole
  - Broadcast/unknown rate limiting
- **You can assign QoS profile when making a permanent, dynamic or blackhole FDB entry by using the CLI configuration command:** create fdbentry

Notes:

Traffic Groupings - Explicit Class of Service

This category of traffic groupings describes what is sometimes referred to as explicit packet marking, and refers to information contained within a packet intended to explicitly determine a class of service. That information includes:

- IP DiffServ code points, formerly known as IP TOS bits
- Prioritisation bits used in IEEE 802.1p packets

An advantage of explicit packet marking is that the class of service information can be carried throughout the network infrastructure, without repeating what may be complex traffic grouping policies at each switch location.

Another advantage is that end stations can perform their own packet marking on an application-specific basis. Extreme Networks switch products have the capability of observing and manipulating packet marking information with no performance penalty.

Extreme Networks products that use "i" chipset support DiffServ capabilities. Products that do not use the "i" chipset s do not support DiffServ capabilities. The documented capabilities for 802.1p priority markings DiffServ capabilities (if supported) are not impacted by the switching or routing configuration of the switch.

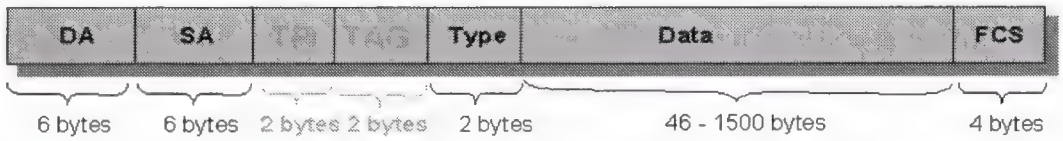
For example, 802.1p information may be preserved across a routed switch boundary and DiffServ code points may be observed or overwritten across a layer 2 switch boundary.

© 2001 Extreme Networks,Inc. All rights reserved

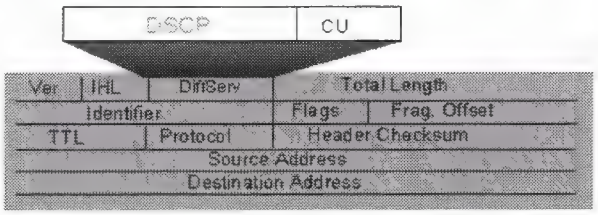
Traffic Groupings

Explicit Class of Service

802.1Q Ethernet Frame



DiffServ IP Packet



- **Also referred to as *explicit packet marking***
  - Refers to information contained within a packet intended to explicitly determine a class of service.
- **Information includes**
  - IP DiffServ code points (IP TOS bits)
  - Prioritization bits used in IEEE 802.1p packets
- **Extreme switches can observe and manipulate packet marking information with no performance penalty**

Notes:

Traffic Groupings - Physical and Logical Groupings

Two traffic groupings exist in this category:

- Source port
- VLAN

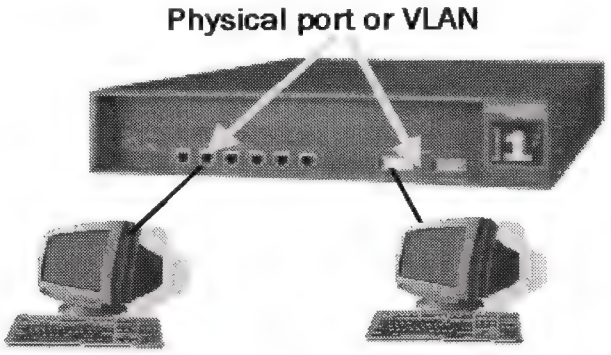
Source Port
A source port traffic grouping implies that any traffic sourced from this physical port uses the indicated QoS profile when the traffic is transmitted out to any other port.

VLAN
A VLAN traffic grouping indicates that all intra-VLAN switched traffic and all routed traffic sourced from the named VLAN uses the indicated QoS profile.

© 2001 Extreme Networks,Inc. All rights reserved

Traffic Groupings

Physical and Logical Groupings



- **Source Port**
  - This implies any traffic sourced from this physical port uses the indicated QoS profile when the traffic is transmitted out to any other port.

- **VLAN**
  - Indicates that all intro-VLAN switched traffic and all routed traffic sourced from the named VLAN uses the indicated QoS profile.

Notes:

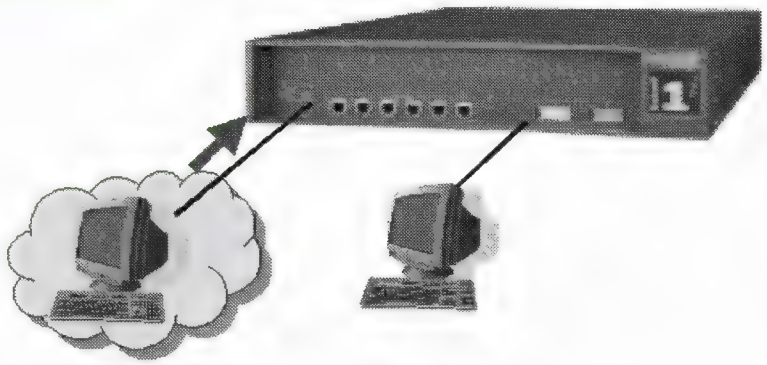
QoS Building Block - QoS Policy

The combination of a traffic grouping and a QoS profile creates a QoS policy.

© 2001 Extreme Networks,Inc. All rights reserved

QoS Building Block

3 – QoS Policy



- **A QoS policy is the combination that results from assigning a traffic group to a QoS profile**
- **Hence in this example:**
  - config vlan dbase_net qosprofile QP4
    - The traffic grouping category of logical traffic grouping i.e. vlan dbase_net was assigned a QoS profile of QP4
    - This is the QoS policy.

Notes:

Steps When Assigning QoS Attributes

The combination of a traffic grouping with a QoS profile results in a QoS policy.

Step 1 - Create a QoS profile
QoS profile — A class of service that is defined through minimum and maximum bandwidth parameters, configuration of buffering, and prioritisation settings. The bandwidth and level of service that a particular type of traffic or "traffic grouping" receives is determined by assigning it to a QoS profile.

Step 2 – Create a Traffic grouping.
These are a classification or traffic type that has one or more attributes in common. These can range from a physical port to a VLAN to IP Layer 4 port information. Traffic groupings are assigned to QoS profiles to modify switch-forwarding behaviour. Traffic groupings transmitting out of the same port that are assigned to a particular QoS profile share the assigned bandwidth and prioritisation characteristics, and hence share the class of service.

Step 3 – Create a QoS policy
Assign one or more traffic groupings to a QoS profile to create a QoS policy.

© 2001 Extreme Networks,Inc. All rights reserved

Steps When Assigning QoS Attributes

- **Configure a default QoS Profile**
- **Assign one or more traffic groupings to a QoS profile to create a QoS Policy**
- **Verify Configuration and Performance**
  - Use the **QoS Monitor** to monitor application performance
  - Determines whether the policies are meeting desired results

Notes:

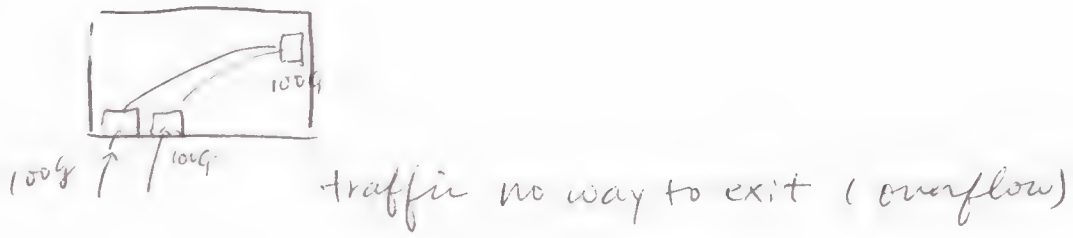
QoS Monitor

The QoS monitor is a utility that monitors the hardware queues associated with any port(s). The QoS monitor keeps track of the number of frames and the frames per second that a specific queue is responsible for transmitting on a physical port.

Two options are available: a real-time display, and a separate option for retrieving information in the background and writing it to the log.

- The real-time display scrolls through the given port list to provide statistics. You can choose screens for packet count and packets per second. The specific port being monitored is indicated by an asterisk (*) appearing after the port number in the display.
- Monitoring QoS in the background places transmit counter and any "overflow" information into the switch log. The log notification appears if one of the queues experiences an overflow condition since the last time it was sampled. An overflow entry indicates that a queue was over-subscribed at least temporarily, and is useful for determining correct QoS settings and potential over-subscription issues.

The QoS monitor can also be used to verify the QoS configuration and monitor the use of the QoS policies that are in place.



© 2001 Extreme Networks,Inc. All rights reserved

QoS Monitor

- **A utility that monitors the hardware queues associated with any port(s).**
- **Keeps track of the number of frames and frames/second that a specific queue is responsible for transmitting on a physical port.**
- **Is available in two options:**
  - Real-time Performance Monitoring
  - Background Performance Monitoring
    - Counter and overflow information is stored in the log file of the switch.

Notes:

Modifying a QoS Policy

If you make a change to the parameters of a QoS profile after a QoS policy has already been formed (by applying a QoS profile to a traffic grouping), the timing of the configuration change depends on the traffic grouping involved.

To have a change in QoS profile effect a change in the QoS policy, the following rules apply:

- For destination MAC-based grouping (other than permanent), clear the MAC FDB using the command clear fdb. This command should also be issued after a policy is first formed, as the policy must be in place before an entry is made in the MAC FDB.
- For permanent destination MAC-based grouping, re-apply the QoS profile to the static FDB entry, as documented. You can also save and reboot the switch.
- For physical and logical groupings of a source port or VLAN, re-apply the QoS profile to the source port or VLAN, as documented. You can also save and reboot the switch.

© 2001 Extreme Networks,Inc. All rights reserved

Modifying a QoS Policy

- **To have a change in QoS profile that will have an effect on the QoS policy, apply these rules:**

- **1 clear fdb**
  - Must be issued after a policy is first formed
  - For permanent destination MAC-based grouping
    - Re-apply the QoS profile to the static FDB entry.
    - Save and reboot the switch

- **2 For physical and logical grouping**
  - Re-apply the QoS profile to the source port or VLAN
    - Save and reboot the switch

Notes:

Summary

You should now be able to:

- Define Policy-Based Quality of Service (QoS)
- Explain types of applications and their QoS requirements
- Define QoS building blocks
- Understand QoS Profiles
- Explain Traffic Groupings and Access Lists
- Define QoS policy
- Explain the QoS CLI configuration commands
- Define the steps in assigning QoS attributes
- Explain QoS policy modification and verification

Successfully complete the lab exercise – optional

© 2001 Extreme Networks,Inc. All rights reserved

Summary

You should now be able to:

- **Define Policy-based Quality of Service (QoS)**
- **Explain types of applications and their QoS requirements**
- **Define QoS building blocks**
- **Understand QoS profiles**
- **Understand traffic groupings and access lists**
- **Understand QoS policy**
- **Explain QoS CLI configuration commands**
- **Define the steps in assigning QoS attributes**
- **Explain QoS policy modification and verification**
- **Successfully complete the lab exercises**

Notes:

Lab 1 – ExtremeWare CLI Familiarization

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student should be able to:

1. Power up and boot a Summit Switch and connect to a Console terminal using a null-modem cable
2. Login into the Switch as an administrator
3. Perform CLI commands – **show switch**, **show management**, **show config**, **show accounts** and **create account**
4. Using the CLI, create a new user account, and login as that user
5. Answer the questions and verify accuracy of the answers at the end of the lab.

MATERIALS REQUIRED:

1. Extreme switch and power cord, and null modem cable
2. PC/laptop as Console terminal with null_modem.nt terminal session on desktop

REFERENCES:

1. Lab procedures from the Student Guide
2. ExtremeWare Software User Guide v. 6.1 (if available)

PROCEDURES:

ASSUMPTIONS:
The switches are in factory default settings and ExtremeWare version is the current version to use prior to performing this lab.

1. Launch the **null_modem.ht** terminal session from the laptop's desktop.

2. Connect a null-modem cable to the serial port on the laptop and the other end of the cable to the console port at the rear of the switch. Power ON the Summit switch.

3. Hit the enter key till the **login** prompt appears. Login as the switch administrator by typing:

login: **admin <cr>**
Password: **<cr>**

4. Examine the Boot messages displayed.

5. From the command prompt, hit the **<TAB>** key. What happened?

_____

6. Display the global switch management information by typing at the CLI prompt: **show switch <cr>** and fill in the switch information below for:

System MAC: 00:01:30:C9:70:00
License:
Software image selected: primary
Software Image booted: primary
Primary software version: 6.2.1b27
Secondary software version: 6.1.7b9
Configuration selected: secondary
Configuration booted: secondary

Lab 1 – ExtremeWare CLI Familiarization

7. Type the CLI command: **show management <cr>**

Indicate below which of the management features displayed are enabled or disabled by default.

	Enabled	Disabled
CLI idle timeouts		✓
CLI Paging:	✓	
CLI configuration logging:	✓	
Telnet access:	✓	
Web access:	✓	
SSH Access:	✓	
SNMP Access:	✓	
RMON polling:		✓
SNMP Traps:	✓	

8. Type the CLI command: **show config <cr>**

Determine how many pre-defined protocols are created when the switch is booted with a default configuration and list them below. RIP. OSPF. ESRP NAT. SNTP

~~Spanning tree protocol~~ / ~~DVMRP~~ / ~~PIM~~ / ~~OSPF~~. ESRP / IPx / NAT

9. Type the CLI command: **show accounts <cr>**

Q: What accounts are created by default on the switch? admin / user

10. Create a new, read-only user account named **Gordon** (capital letter "G") and assign it the password **extreme1** using the CLI command **create account { admin | user } <user name>.**

What does the "*" preceding the command prompt indicate after the above command was executed?

save

11. Logout without saving configuration changes, and log back in as **gordon** (lower case "g"). Were you able to? no. Now login as **Gordon**.

Q: Are account parameters case-sensitive? yes

Login as system administrator and delete the user Gordon.

Q: What is the command to delete user Gordon? delete account Gordon

12. Now type the CLI command **show session**

Q: What is the difference between **show accounts** and **show session** commands?

13. Before logging out, be sure to save any of your configuration changes by typing:

Save <cr> Do you want to save to the primary configuration database? **Y <cr>**

This completes Lab1 – CLI Familiarization.

Lab2 – More CLI – Image & Configuration

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Understand the need to configure VLAN **default** by assigning an IP address to it.
2. Configure the PC/Laptop and connect to the switch.
3. Utilize a TFTP Server to download software image on to the switch using CLI commands **download image** and **use image**
4. Verify that the download was successful using the CLI command **show switch**.
5. Utilize the TFTP Server to download a modified configuration file using the **upload config, download config** and **use config** CLI commands

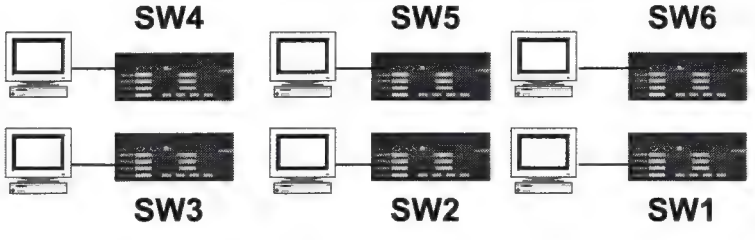
MATERIALS REQUIRED:

1. Extreme switch, power cord and a null-modem cable
2. PC/laptop with RJ-45 cable

REFERENCES:

1. Lab2 procedures from Training Guide
2. ExtremeWare Software User Guide 6.1 (if available)

PROCEDURES: (This Lab is performed on all Switches)



1) Turn on your switch and logon as administrator.

2) Examine the VLAN **default** that you will configure using the **show vlan** command.

Q. Does **default** have an IP address? No

Q. Which ports belong to the pre-configured VLAN **default**? 3/8

3) Assign the IP address of 10.0.4.**n**/24, to VLAN **default** (**n** = switch station number) using the CLI command: **config DEFAULT ipaddress <ip_address/mask>**

What command will you use to verify that the change has been made to Vlan default?

Show VLAN

4) Configure the PC/laptop with :

IP Address	= 10.0.4.10**n** (**n** = switch station number):
IP Mask	= 255.255.255.0
Gateway	= <none>

Lab2 – More CLI – Image & Configuration

5) Connect the PC/laptop to one of the switch port using a straight-thru cable.
Do you have a Link OK signal on the port? yes

Q: Does it matter in which port the PC/laptop is connected to? Explain.

No, all ports are on default vlan

6) Launch the TFTP server from the <tftpd32> icon on the PC/Laptop's desktop.

Record the TFTP Server IP Address. 10.0.4.104

7) Display the global switch information.

Q: What versions of software are currently installed on the switch, and in which locations.

6.2.1b27 (Primary) 6.1.769 (secondary)

8) Download a new version of the switch image from the TFTP Server (laptop) to the switch:

a. Go to the PC/laptop's **C:\tftpfile** Folder containing several software image files. Select a lower revision image file to download, i.e. **v617b9.xtr**

b. Check to see that the directory settings for the TFTP Server is **c:\tftpfile**

c. With the TFTP Server running, execute the CLI command to download the software image into the secondary container using:

download image <tftp_server ip_address> <_image version> secondary

Are you sure you want to overwrite the secondary image (Y/N) **Y** **<cr>**

Observe the messages displayed from the TFTP Server Screen.

9) Confirm that the download was successful using the CLI **show switch**.

Q: What version of the software is now running on the switch? 6.2.1b27
Q. What version of the software is selected? secondary

10) Change the selected boot image to the newly downloaded file using the CLI command:

use image secondary **<cr>**

Q: What version of the software is now running on the switch? 6.2.1b27
Q. What version of the software is selected? secondary

11) Execute the CLI command **reboot**. Answer **Y** to the message:

The Configuration database has been changed. Do you wish to save these changes…

Q: What version of the software is now running on the switch for:

Software Image selected? secondary

Software Image Booted? secondary

Lab2 – More CLI – Image & Configuration

12) Change the selected boot image back to the original (primary) and reboot the switch.

What command will you use? use image primary

13) Perform an upload config command to the TFTP Server using the command:

upload config <TFTP Server IP_Address> <C:\..\< new_config_name.cfg>

Example:
upload config 10.0.4.101 newfile.cfg <cr>

14) Edit the configuration file by going to a DOS prompt and typing **edit <newfile.cfg>**

Change the System Name in the line that says **configure snmp sysName "Summit1i"** to something unique, e.g. **your_name _Switch**.

Save the file as a text file. Example: **<filename>.txt**

15) Download the edited configuration file using the CLI command:

download config <TFTP Server IP_Address> <text file name> <cr>

16) **REBOOT** when the switch prompts you to and login in.

Do a **show switch** command.

17) Note the **sysName** on the CLI command prompt. Did it change? yes

18) Examine the configuration selected and note what is displayed.

What is displayed in the configuration selected field? secondary
What is displayed in the configuration booted field? "

What happens if the configuration is not saved? Which configuration is used on boot?

primary

19) Logout of the Console Terminal. Do **not** save the configuration and turn off the switch.

This completes Lab2 – More CLI – Image and Configuration Files

Lab3 – ExtremeWare VISTA Familiarization

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student should be able to:

1. Access the ExtremeWare Vista device-management software using a standard Web browser
2. Be familiar with the CLI subset of commands accessible in ExtremeWare Vista
3. Perform a configuration change under Support and perform a TFTP download
4. Verify that the command was executed successfully, just like a CLI command

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables and null modem cable as required.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:

ASSUMPTION: Lab2 exercise has been completed and that at least one VLAN on the switch has been assigned an IP address and the PC/Laptop running the browser has been configured with an IP Address.

1. Power on the switch. Connect the PC/Laptop NIC to one of the free port on the Summit switch. Reboot the laptop, login and then access your browser. (e.g. Netscape Communicator)

2. Enter the following at the URL field to access the default VISTA home page:

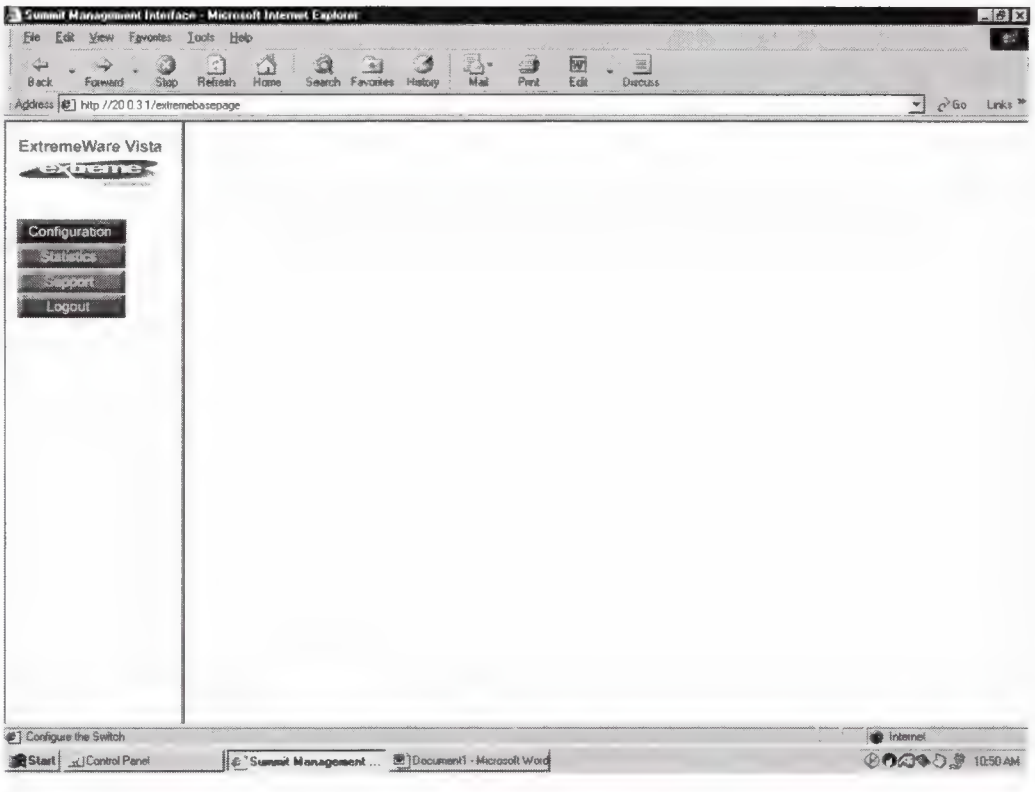
   http:// <switch_ipaddress>

   The Logon screen is displayed. Click on **Logon**.

Lab3 – ExtremeWare VISTA Familiarization

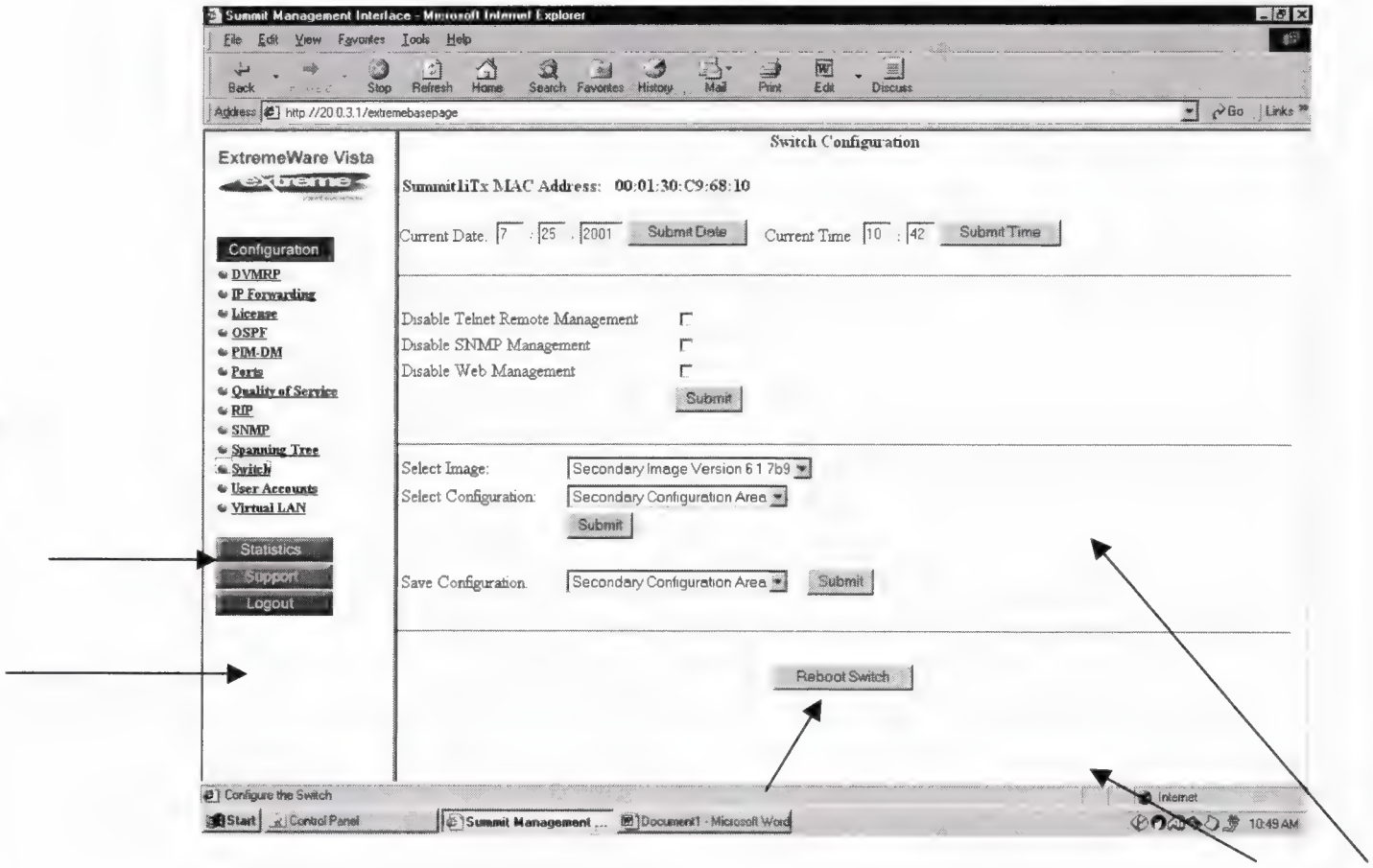
3. Login as the switch administrator by typing: **admin** with no password.

4. Examine the ExtremeWare Vista home page that is displayed. Click on **Configuration – Switch.** Note that the browser screen displayed is divided into 3 sections as follows:



Lab3 – ExtremeWare VISTA Familiarization

5. Which are the Task Frame, Task Tab, Content Frame and Standalone Button? Use the arrows to label each.



6. Click on the task tab – **Configuration**. What Options are displayed?

DVMRP
IP forwarding
License
OSPF
PIM-DM
Ports
Quality of service
RIP
SNMP
Spanning tree
Switch
User Accounts
Virtual LAN

Lab3 – ExtremeWare VISTA Familiarization

7. Click on the task tab – **Statistics**. What are the Options displayed?

Event Log
FDB
IP ARP
IP configuration
IP route
IP statistics
Ports
Port Collisions
Port errors
Port Utilization
RIP
Switch

8. Click on the task tab – **Support.** What are the Options displayed?

Help
TFTP Download
Contact Support
Email Support

Click on each of the options to observe what can be accessed.

9. Using VISTA displays, determine what the equivalent is for the following CLI commands:

- Show Switch
- Show Port Utilization
- Show IP Config
- Show Accounts
- Config Accounts
- Show Vlan

V6.1.9b22 xfr
V6.1.9b22 tftp

10. The only configuration change you will do for this exercise is a TFTP download.

    Using **VISTA –> Support –> TFTP Download**, change the current image file loaded on the switch secondary location to the current version (ex. EW 6.1.7+) . Ensure that the TFTP Server is running.

    Note the messages displayed at the top of the TFTP Download screen as the download is in progress.

11. When finished with the TFTP download, do a CLI show switch equivalent to verify that both primary and secondary software image locations contain version EW 6.1.7+.

12. When done, click on task tab – **Logout** and power off the switch.

This completes the Lab3 – ExtremeWare VISTA Familiarization.

Lab 4 – Accessing The BootROM Menu

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student should be able to:

1. Determine when to interact with the BootROM menu for disaster recovery – such as when the switch hangs, utilize this procedure to communicate with the switch.
2. Describe how to access the BootROM Menu
3. List the available Boot Option Commands with the BootROM menu and know when to use them.

MATERIALS REQUIRED:

1. Extreme switch, power cord and null-modem cable
2. PC/Laptop and network cable

REFERENCES:

1. Lab procedures from the Training Guide
2. ExtremeWare Software User Guide 6.1 (if available)

PROCEDURES:

ASSUMPTION: PC/Laptop is connected as a terminal to the console port of the switch and displays a terminal emulation screen for switch CLI interface.

1. With the switch powered up, from the terminal emulation screen, logon as administrator.

2. Simultaneously power cycle the switch while depressing the <spacebar> on the terminal's keyboard.

3. Watch the screen for the BootROM> prompt to appear, then release your hold on the <spacebar>.

```
Boot Module 27 JUL 00 v6.5
==========================
Memory Size: 08000000

Press spacebar for boot menu
BootROM->
BootROM->
BootROM->
BootROM->
BootROM->
BootROM->
BootROM->
BootROM->
BootROM->
BootROM->
BootROM->
BootROM->
BootROM->
BootROM->
```

Lab 4 – Accessing The BootROM Menu

4. Press "h" for a display of a simple help menu.

```
BootROM->h

1: Select primary code image
2: Select secondary code image
3: Select primary configuration
4: Select secondary configuration
b: Change baud rate
d: Force default configuration
f: Boot on board flash
h: Help
k: Erase selected configuration
p: Boot PCMCIA card
s: Load code image from serial port using XMODEM

BootROM->
```

5. Interaction with the BootROM menu is only required under special circumstances and should be done only under the direction of the Extreme Networks Customer Support. The necessity of using these functions implies a non-standard problem requiring Extreme assistance.

6. This lab is for general information only.

This completes the Lab4 – Accessing BootROM for Disaster Recovery

Lab5 – Port and Load Sharing Configuration

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Setup a network and be familiar with port configuration commands.
2. Display switch port configuration using CLI command – **show port config**
3. Create a four-port load-share group using port 1 of the Summit48 switch as master via the CLI command – **enable sharing <port_number> grouping**
4. Understand and verify that the load share procedure exercises by introducing a continuous data stream via the wsttcp.exe utility and examining port statistics.

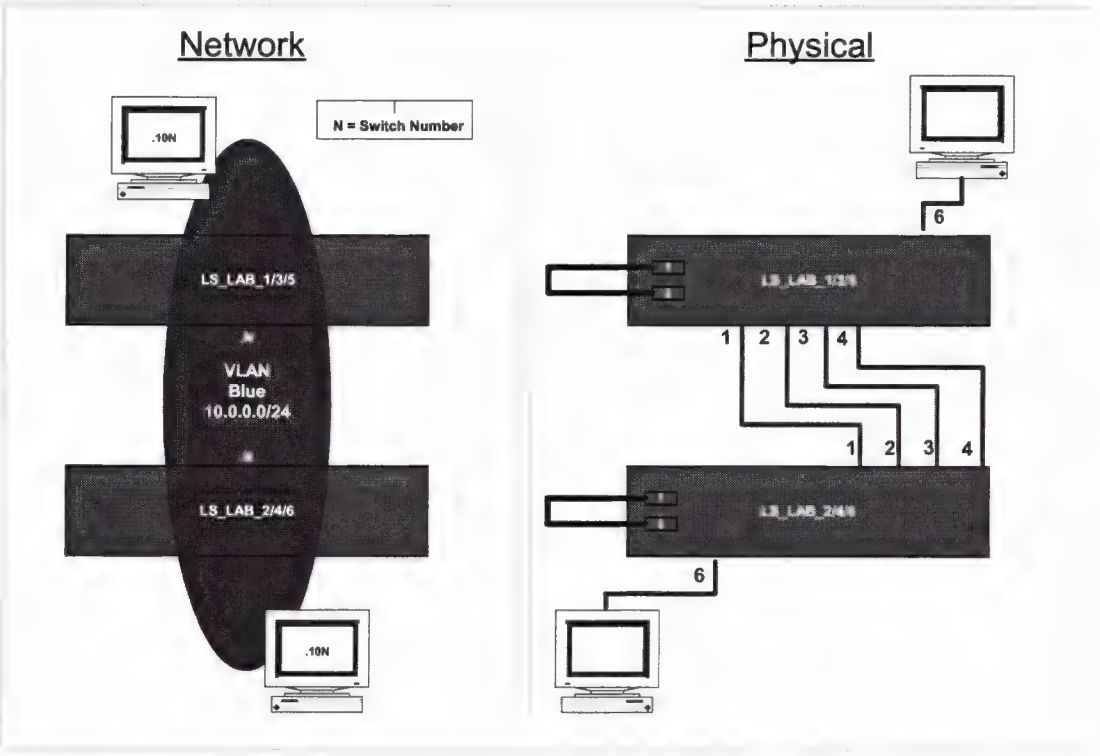
MATERIALS REQUIRED:

1. Extreme switch and power cord, and null modem cable
2. PC/laptop as Console terminal with null_modem.nt terminal session on desktop
3. Straight-thru, cross-over cables as required
4. **wsttcp.exe utility** on the PC/Laptop – as continuous data stream supplier

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide v. 6.1 (if available)

PROCEDURES:



1) Clear the switch of all old configuration information with the command **unconfig sw all**

2) Delete all ports from VLAN **default** .

Lab5 – Port and Load Sharing Configuration

3) Name the switch according to the following template: LS_LAB_**<switch number>** using the command: **config snmp sysname LS_LAB_#<cr>**

4) Using a fiber cross-over patch cable, connect port 7 to port 8. (Assuming Summit 1i's are used, otherwise, pick any two Fiber-based Gig ports).

What color are the status lights for ports 7 and 8? green

What does the status lights indicate?

There is traffic going through

5) Disconnect the patch cable from port 7. Turn off auto-negotiation on port 7 using the command: **configure port 7 auto off duplex full**. Reconnect the patch cable.

What is the status light on port 7? green

What is the status light on port 8? no light

Will this connection be able to pass data?

no traffic

6) Disconnect the patch cable from both ports 7 and 8

7) Display the port configuration for ports 1-4. Use the command:

show ports 1-4 configuration

What is the load share status for these ports?

no load sharing

8) Create a four-port load-share group for ports 1-4 with port 1 as the master using the CLI command **enable sharing <master port number> grouping <port_list>**

9) Display the port configuration for ports 1-4 using the CLI command **show ports <portlist> config**.

What is in the Load Share Master column display now?

There is load sharing now

10) Create the VLAN **blue**, give it an IP address in the 10.0.0.**N**/24 network using the number of your **Switch_N**, and assign port 6 and 1-4. The following CLI commands for these are:

What error message do you get after entering this command?

Port 2 is in load-sharing mode.

Why did you get this error? Perform all config changes to the logical link

Port 1 is master port,

all you have to do is only assign port 6 and 1.

→ config blue add ports 6, 1

Lab5 – Port and Load Sharing Configuration

11) Configure the laptop with the following parameters:

IP Address	= 10.0.0.10**N**	; *Where N = Switch Number*
IP Mask	= 255.255.255.0	
Gateway	= <none>	

12) Using a CAT5 cross-over patch cable, connect port 1, 2, 3, and 4 to your partner switch' ports 1, 2, 3, and 4 sequentially. Using a CAT5 straight-through cable, connect the laptop to port 6.

Before proceeding, confirm that your partner switch team has also completed step (12)

13) From your laptop, launch the **wsttcp.exe utility** in a DOS window from **c:\temp** directory.

wsttcp -t -u -n1000000 10.0.0.N *Where N= Switch number of your partner switch*

This will initiate a continuous data stream directed at your partner switch's IP interface.

Coordinate steps (14) through (17) with your partner switch team.

14) Display the port statistics for ports 1-6 using the CLI command **show ports <port_list> stats**.

Which ports are showing traffic?

~~1~~ ~~5~~ 2, 6

What is the significance of the receive data reported on port 6?

receive the traffic from switch team

15) You can observe how load sharing operates when you disconnect the cable from port 4, then 3, then 2 respectively. What have you observed?

disconnect 4 → 3. 6

disconnect 3 → 2.

2 → 1

This completes Lab5 – Port and Load Sharing Configuration Lab

Lab6–FDB Configuration Familiarization

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Be familiar with the CLI commands for configuring FDB entries and their effect on the network to know how to display the FDB contents.
2. Utilize the FDB configuration CLI commands: **create fdbentry; config fdb aging time**; **show fdb**, and **clear fdb**

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables and null modem cable as required.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:

1) Clear the switch of all old configuration. Delete all ports from VLAN **default**. Name your switch as **FDB_Lab#** where **#** is your switch number.

2) Create a permanent fdb entry and blackhole it for MAC address: 00:01:30:22:a9:01 associated with VLAN **default**.

3) Display the switch's forwarding database. Is the entry you just created displayed ?

~~No~~ yes

4) Do a **clear fdb** and see if this entry can be removed. Explain why or why not?

No, it is static MAC
how to delete it ? Delete Fdb entry 00:01:30:22:a9:01

5) Network and configure several switches together including your own so your laptops and switches can see each other. default

Practice on trying to block each other's pings using the **create fdbentry** command. Practice using other FDB configuration CLI commands you already learned.

This completes Lab6 – FDB Configuration Familiarization

Lab7 – Port-Based VLAN Configuration I

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Utilize the CLI commands for bridging and VLAN configuration – **show vlan, create vlan, configure vlan**.
2. Create and configure a new VLAN named Redish and Blue
3. Use PING to verify connectivity to the VLAN interfaces, and devices connected to it.
4. Understand how ping works across an L2 boundary in our switch.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables and null modem cable as required.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:

1) Clear the switch of all previous configuration using CLI command **unconfig sw all** and type **Y** to confirm and reboot.

2) Delete all ports from VLAN **default** by entering: **config default delete port all.**
Do a **show vlan <cr>** *No ports should be configured by now.

3) Name the switch VLAN1_LAB_<**switch number**> using the CLI command:
config snmp sysname VLAN1_LAB_N <cr>

4) Create the VLAN **redish**, give it an IP address in the 10.0.0.**N**/24 network using N as the number of your **Switch**, and assign port 1. Do a SHOW VLAN **redish** to see the changes made:

create vlan redish
config redish ipaddress 10.0.0.N/24
config redish add port 1
show vlan redish

5) Create the VLAN **blue**, give it an IP address in the 20.0.0.**N**/24 network, and assign port 6. Do a SHOW VLAN **blue** to see the changes made.

6) Save this configuration in the Primary location and then select PRIMARY configuration as the default when the switch is rebooted.

7) Configure and restart the PC/laptop with the following parameters:

Lab7 – Port-Based VLAN Configuration I

IP Address = 20.0.0.10**N** ; where **N = Switch Number**
IP Mask = 255.255.255.0
Gateway = **<none>**

8) Using a cross-over cable, connect port 1 to port 2.
Using a straight-through cable, connect your PC/laptop to port 6.

9) From the console, ping the switch interfaces, 10.0.0.**N** and 20.0.0.**N**.

Did both interfaces respond to the ping? ~~no~~ yes

10) Display the IP configuration information for VLAN **redish** using the CLI command: **show ipc <vlan_name>**. Look at the Router Interface # on Vlan.

What is the interface state for this VLAN? UP or DOWN? up

11) Disconnect the cross-over cable from port 2. Display the IP configuration information for VLAN **redish** again.

Has the state changed after disconnecting the cross-over cable? VLAN interface is down

12) With the cross-over cable still disconnected, ping the 10.0.0.N interface. What happened?

no response

13) Re-connect the cross-over cable you removed in Step 11.

14) From the laptop, open a DOS window, ping the **blue** interface, 20.0.0.N
Does this interface respond to the ping? ~~no~~ yes

15) Now, ping the **redish** interface, 10.0.0.N.
Does this interface respond to the ping? No

Why can the laptop ping the VLAN **blue** but not VLAN **redish**?

Because my workstation are on the same ~~switch~~ VLAN Blue

16) Reconfigure your laptop to use the **blue** interface as gateway:

IP Address = 20.0.0.10**N** ; where **N = Switch Number**
IP Mask = 255.255.255.0
Gateway = 20.0.0.**N**

17) From the laptop, ping the **redish** interface 10.0.0.N again.
Does this interface respond to the ping? yes

If this is a layer-2 only configuration and elements from dissimilar broadcast domains cannot normally communicate, why is the laptop now able to ping the the vlan it does not connect to?

use the interface 20.0.0.4 (as a gateway/or route) to route the packets to Destination

18) Save your current configuration in preparation for the next lab exercise.

This completes the Lab5 –Port-based VLAN Configuration I

Lab8– Port-based VLAN Configuration II

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Expand the previous lab exercise to include spanning across switches
2. Utilize the CLI command **show fdb**
3. Verify that there are instances of the broadcast MAC address FF:FF:FF:FF:FF:FF for each VLAN.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables and null modem cable as required.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:

1) Continuing with the previous Lab5, you will pair with a partner switch in this lab. SW1 with SW2, SW3 with SW4 and SW5 with SW6.

2) Add port 3 to VLAN **redish** and port 4 to VLAN **blue**.

3) Using a cross-over cable, connect port 3 of your switch to port 3 of your partner switch.

4) Using a second cross-over cable, connect port 4 of your switch to port 4 of your partner switch.

5) Save this configuration to the Primary location.

6) From the switch console, ping both the 20.0.0.N **(blue VLAN)** and the 10.0.0.N (**redish VLAN)** interfaces on the other switch.

Did the two interfaces respond to the ping? _____

Lab8– Port-based VLAN Configuration II

7) From the PC/laptop at a DOS prompt, attempt to ping the other laptop in the 20.0.0.0/24 (**blue**) subnet. Did the host respond to the ping? Yes.

8) Display the switch's forwarding database using the CLI command **show fdb**.

How many entries are there for the broadcast MAC address?

4

9) You can expand this exercise by attempting to network all 6 switches and see if you can ping all 10 interfaces and 5 additional laptops. Ensure you have continuity with both **blue** and **redish** VLANs.

10) When you are successful with step 9, attempt to move the laptops of SW2, SW4 and SW6 to belong to the redish VLAN instead of the blue. How will this be accomplished?

11) Save your configuration in the primary location.

This completes the Lab8 – Bridging and VLAN Configuration – II

Lab9 –VLAN Configuration III with Tags

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Utilize the CLI commands–**create vlan, configure vlan tag; config vlan add po tagged**. Configure a VLAN and assign an explicit tag.
2. Verify that the interfaces are working using the tagged VLAN
3. Understand how to create separate tags for each broadcast domain and propagate them across the switches
4. Learn how broadcast traffic can better be managed.

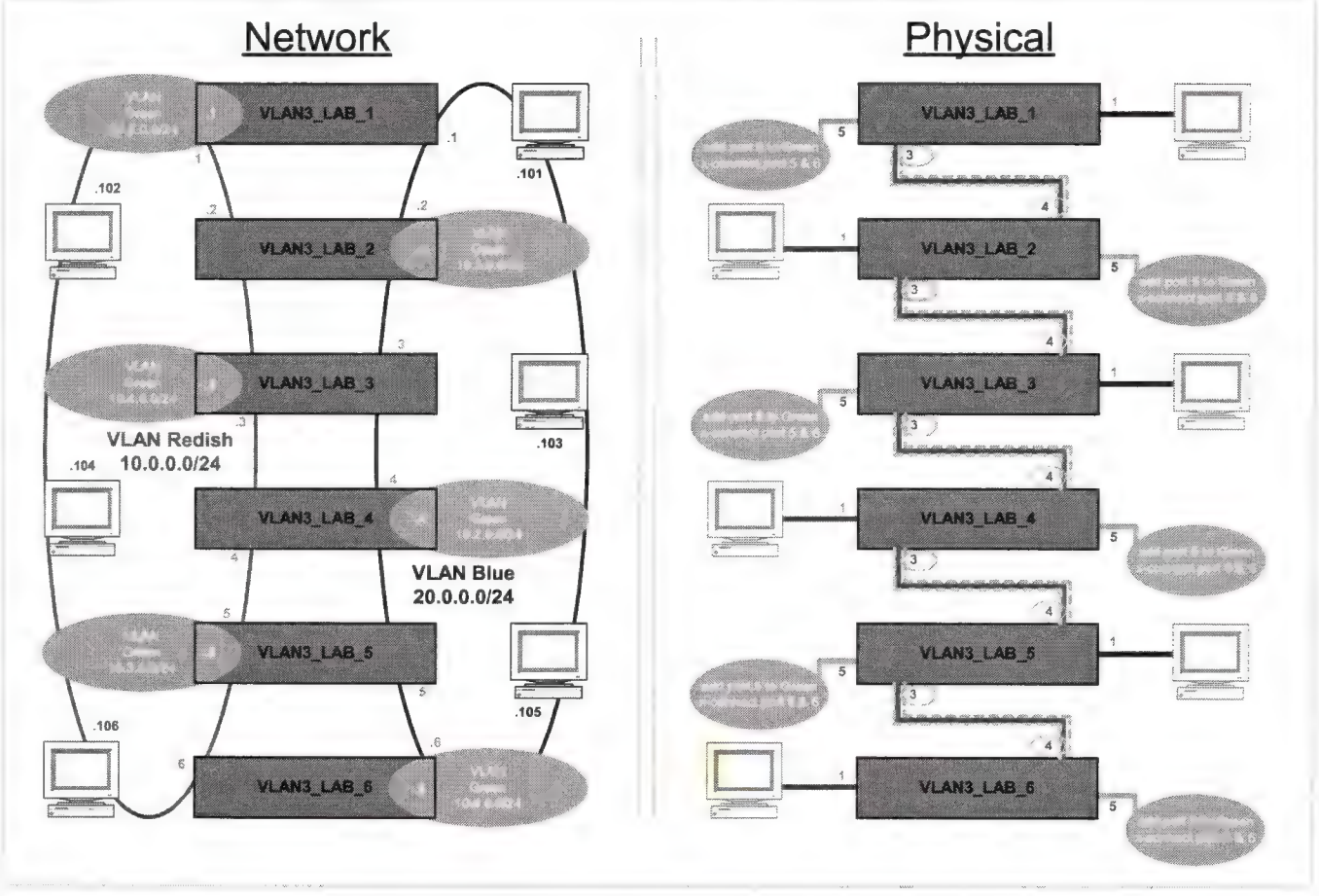
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables and null modem cable as required.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:



Lab9 –VLAN Configuration III with Tags

1) Clear the switch of all old configuration and delete all ports from VLAN **default**. Name the switch according to the following template: VLAN3_LAB_<**switch number**>. Remove any cables connected on the switches from previous labs.

2) Create the VLAN **redish**, give it an IP address in the 10.0.0.**N**/24 network where N is your switch number.

   Create the VLAN **blue**, give it an IP address in the 20.0.0.**N**/24 network.

3) Add port 1 to VLAN **blue** for SW1, SW3 and SW5.

   Add port 1 to VLAN **redish** for SW2, SW4 and SW6.

4) Configure and restart the PC/laptop with the following parameters:

   For SW1, SW3 and SW5

   IP Address = 20.0.0.10**N** ; where **N = Switch Number**
   IP Mask = 255.255.255.0
   Gateway = 20.0.0.**N**

   For SW2, SW4 and SW6

   IP Address = 10.0.0.10**N** ; where **N = Switch Number**
   IP Mask = 255.255.255.0
   Gateway = 10.0.0.**N**

5) Using a straight-through cable, connect the PC/Laptop to port 1 of vlan **blue** (for SW1, SW3 and SW5); and port 1 of vlan **redish** (for SW2, SW4 and SW6).

   Using cross-over cables, connect port 3 of SW1 to port 4 of SW2, connect port 3 of SW3 to port 4 of SW4; connect port 3 of SW4 to port 4 of SW5; connect port 3 of SW5 to port 4 of SW6.

6) Add port 3 and port 4 to vlan **blue.**

7) Add port 3 and port 4 to vlan **redish**. Can you do it? Explain why?

   No, you can't assign two VLANs for one particular port.

8) Do a show vlan **blue**. Does VLAN **blue** have a tag? no

   Do a show vlan **redish**. Does VLAN **redish** have a tag? no

Lab9 –VLAN Configuration III with Tags

9) Configure VLAN **redish** with the explicit tag **10.**

10) Add port 3 and port 4 to VLAN **redish** as tagged ports using the CLI command:
config <vlan_name> add port <port_list> **tagged**

Were you able to do it this time? yes

11) Display the configuration information for VLAN **blue** and VLAN **redish.**
How many ports are now members of VLAN **blue** and VLAN **redish**? Which ones are tagged/untagged?

Blue 3 4 (un) tagged redish 3 4 (tagged) 1 (untag)

12) From the switch console, ping both the **redish** and **blue** interfaces on the other five switches.
Did all ten interfaces respond to the ping? yes

13) From the laptop, ping the laptops belonging to the 20.0.0.0/24 (**blue**) subnet. Did they respond? no

Now, ping the other laptops in the 10.0.0.0/24 (**redish**) subnet. Did they respond?

yes.

14) Create the VLAN **green** and configure it with an explicit tag of **20**.

15) Assign an IP address in the network specified below for each switch:

Switch	**IP Address**	
SW1 & SW4	10.2.0.**N**/24	; **where N = switch number**
SW2 & SW5	10.3.0.**N**/24	
SW3 & SW6	10.4.0.**N**/24	

16) Configure VLAN green with port **5** as an untagged port, and port **3** and **4** as tagged ports.

17) Using a cross-over cable, connect port 5 to 6.

18) From the switch console, ping the **green** interfaces on the other five switches.
Do all five interfaces respond to the ping? no

What is significant about the six **green** VLANs current configuration and broadcast traffic?

They are on different subnets.

This completes Lab9 – VLAN Configuration III with Tags.

Lab10 –MAC-Based VLAN Configuration

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Be familiar with the CLI commands for configuring MAC-based VLANS, – **enable mac-vlan mac-group, config mac-vlan add mac-address, show mac-vlan**
2. Create, enable and associate MAC address to a MAC based VLAN.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables and null modem cable as required.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:

1) Clear the switch of all old configuration. Delete all ports from VLAN **default**. Name your switch as **MAC_Lab#** where **#** is your switch number.

2) Create three VLANs named sales, finance and engineering.

3) Enable port 1-4 to use the MAC-based VLAN algorithm. This port should not be a member of any VLAN. Use the grouping of ANY.

   Display the MAC-based Vlan configuration of vlan **MacVlanDiscover** using the CLI command: **show mac**

   What did you observe?

   All ports are ~~"group"~~ in one "group"

4) Associate/add each MAC address to the MAC-based VLAN using the CLI command **config mac-vlan using the information below:**

Mac	**Vlan**	**Group**
Any	default	any
00:00:11:11:22:22:	sales	1
00:00:22:22:33:33:	finance	2
00:FF:11:22:33:44:	engineering	3

   Display the MAC-based VLAN configuration & database using the command:**show mac.**

   Do a show vlan detail and examine the vlan **MacVlanDiscover**
   What did you observe?

This completes Lab10 – MAC-based VLAN Configuration.

Lab11 –vMAN Configuration Familiarization

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Be familiar with the CLI commands for configuring vMANs, **–configure dotq ethertype; configure jumbo-frame size, enable jumbo frame ports**.
2. Perform a practice configuration based on diagram shown.

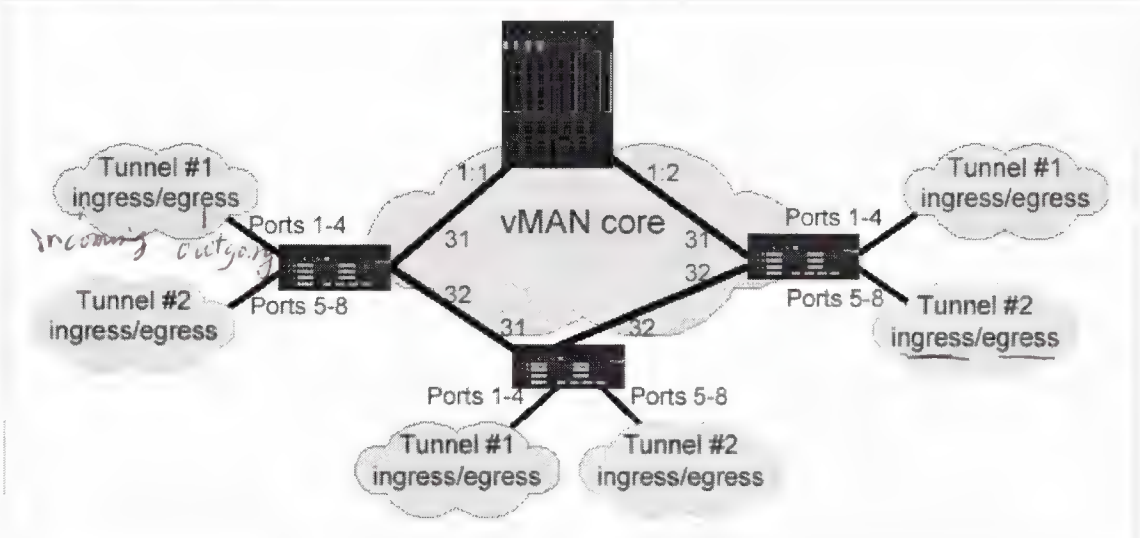
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables and null modem cable as required.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:



1) Assume that your switch will connect to Black Diamond, configure your switch to provide the vMAN tunnels as shown. If your switch does not have any ports 31 and 32, feel free to substitute the port numbers. Parameters for your configuration exercise are as follows:
   i. Vlan tunnel names: **Tunnel1** and **Tunnel2**
   ii. Tunnel1 configured with Tag 50
   Tunnel2 configured with Tag 60
   iii. Ethertype to use is 9100
   iv. Use ports 7-8 to connect to the BD
   v. Use Port 1-2 as ingress/egress for Tunnel1
   vi. Use Port 3-4 as ingress/egress for Tunnel2
   vii. Jumbo-frame size 1530

This completes Lab11 – VLAN Configuration III with Tags.

Lab12 – Spanning Tree Configuration

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Setup a network of switches and configuring vlans to create broadcast storms.
2. Configure the network with spanning tree using the CLI commands – **enable s0**, **show s0**, **show stpd s0 ports <list>**
3. Understand how to determine which switch is the root bridge, port states and other spanning tree parameters.

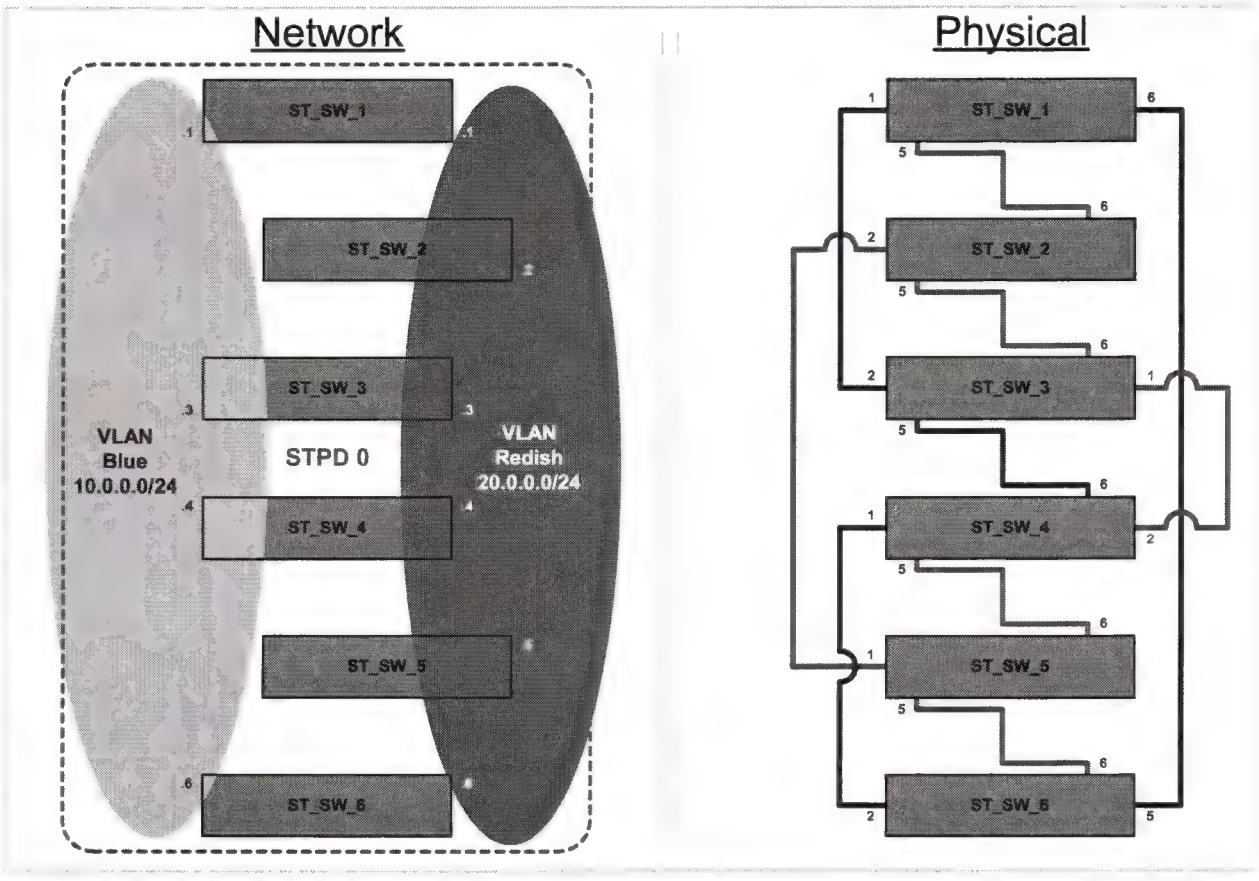
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required and null modem cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:



*NOTE: Only 4 of the 6 switches will create and configure Vlan **blue** (Switch 2 and Switch 5 will not). All 6 switches will create and configure a Vlan **redish***

Lab12 – Spanning Tree Configuration

Remove all cable connections on the switch if any. Clear the switch of all old configuration information and then issue a reboot. Delete all ports from VLAN **default**.

1) Create VLAN **redish**, give it an IP address in the 20.0.0.**0**/24 network and assign ports as follows:

	VLAN **redish**
SW1	5
SW2	2, 5 & 6
SW3	1 & 6
SW4	2 & 5
SW5	1, 5 & 6
SW6	6

2) Create the VLAN **blue**, give it an IP address in the 10.0.0.**N**/24 network, and assign as follows:

	VLAN **blue**
SW1	1 & 6
SW2	none
SW3	2 & 5
SW4	1 & 6
SW5	none
SW6	2 & 5

3) Using cross-over cables, connect the switches as shown in the network topology and below:

SW1 → port 1 → SW3 port 2
port 5 → SW2 port 6
port 6 → SW6 port 5

SW2 → port 2 → SW1 port 1
port 5 → SW3 port 6
port 6 → SW1 port 5

SW3 → port 1 → SW4 port 2
port 2 → SW1 port 1
port 5 → SW4 port 6
port 6 → SW2 port 5

SW4 → port 1 → SW6 port 2
port 2 → SW3 port 1
port 5 → SW5 port 6
port 6 → SW3 port 5

SW5 → port 1 → SW2 port 2
port 5 → SW6 port 6
port 6 → SW4 port 5

SW6 → port 2 → SW4 port 1
port 5 → SW1 port 6
port 6 → SW5 port 5

4) Observe the switch port LEDs as soon as all cables are connected.

What do you think is happening? Looping.

5) Examine the default STPD S0 and verify the STP parameters using the CLI command: **show stpd s0**

STP is disabled

Lab12 – Spanning Tree Configuration

6) Wait for all switches to be configured. Do not enable spanning tree unless the instructor tells you do so.

7) Enable spanning tree on each switch by issuing the CLI command: **enable s0**

Did all the broadcast storms disappear? Yes.

8) Which switch is the root-bridge? How would you determine this?

show STPD S0 00:01:30:C9:70:00

9) Do a **show stpd s0 ports <list>** for all ports you configured. Examine the STP Port State for each port. Determine which ports are in the forwarding and which ones are blocking and list them below:

		FORWARDING	BLOCKING
SW1 →	port 1 →		
	port 5 →		
	port 6 →		
		FORWARDING	**BLOCKING**
SW2 →	port 2 →		
	port 5 →		
	port 6 →		
SW3 →	port 1 →		
	port 2 →		
	port 5 →		
	port 6 →		
SW4 →	port 1 →		
	port 2 →		
	port 5 →		
	port 6 →		
SW5 →	port 1 →		
	port 5 →		
	port 6 →		
SW6 →	port 2 →		
	port 5 →		
	port 6 →		

10) With this setup, Spanning Tree is enabled and working.

The instructor will now map the blocked ports as reported by each lab station.

Is the **blue** broadcast domain contiguous or partitioned? Contiguous

Is the **red** broadcast domains contiguous or partitioned? _____

11) The team on ST_LAB_2 will now change their spanning tree bridge priority to **100** using the CLI command: **config stpd s0**

Lab12 – Spanning Tree Configuration

Display the spanning tree information for the domain **S0**.

Which switch is now the root bridge? SW6

1) Display the state of the switch connected ports whether forwarding or blocking.

		FORWARDING	BLOCKING
SW1 →	port 1 →		
	port 5 →		
	port 6 →		
SW2 →	port 2 →		
	port 5 →		
	port 6 →		
SW3 →	port 1 →		
	port 2 →		
	port 5 →		
	port 6 →		
SW4 →	port 1 →	✓	
	port 2 →	✓	
	port 5 →		X
	port 6 →	✓	
SW5 →	port 1 →		
	port 5 →		
	port 6 →		
SW6 →	port 2 →		
	port 5 →		
	port 6 →		

2) *The instructor will update the map of blocked ports as reported by each lab station.*

Is the **blue** broadcast domain contiguous or partitioned? _____

Is the **red** broadcast domains contiguous or partitioned? _____

If the broadcast domains cannot be 'healed' by changing the root bridge, how can this network design be made to work without changing the VLAN configuration?

_____

14) Create a new spanning tree domain, **S1**.

15) Move the VLAN **redish** into the new spanning tree domain **S1** using the CLI command **config stpd <stpd_name> add vlan**.

16) On the instructor's direction, enable the spanning tree protocol for the domain **S1**.

_____

Lab12 – Spanning Tree Configuration

17) Display the spanning tree information for the domain **S0 and S1**

18) Which switch is the root bridge for each STPD?

		Root Bridge
STPD S0	➔	_____ (SW6)
STPD S1	➔	myself. (SW4)

Are there any layer-2 loops (broadcast storms)?

no

19) Are the VLANs contiguous or partitioned? _____

This completes the Lab 12 – Spanning Tree Configuration

Lab13 – IP Forwarding Configuration

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Create a network of two vlans and display the IP route table on the switch using the CLI command - **show iproute**
2. Enable IP forwarding for vlans using the CLI command – **enable ipforwarding**
3. Display the forwarding database, ARP table and IP forwarding database with the CLI commands – **show fdb, show iparp, show ipfdb**.
4. Add/delete a static route using CLI command – **config iproute add** and **config iproute del**
5. Clear the forwarding database and IP forwarding database using CLI command – **clear fdb** and **clear ipfdb**.
6. Understand how to configure IP Forwarding and Routing procedures on the switch.

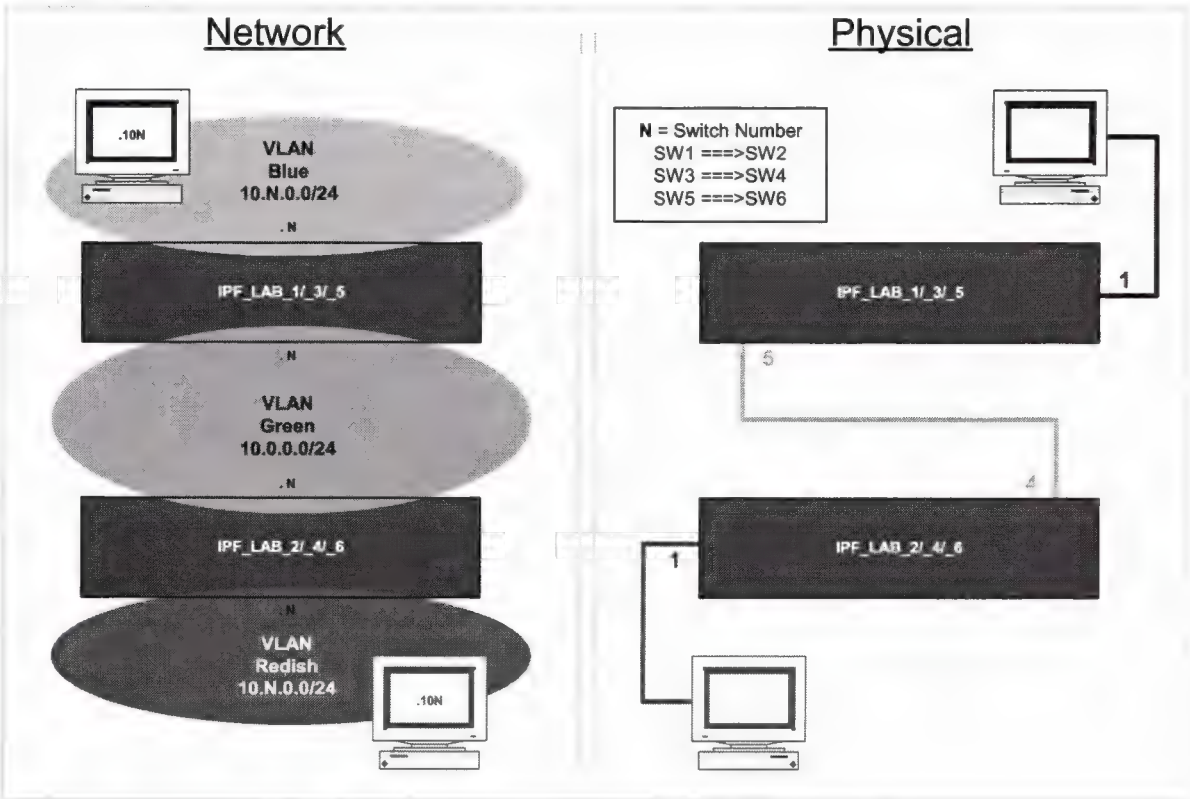
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:



Lab13 – IP Forwarding Configuration

1) Clear the switch of all old configuration information with the command **unconfig sw all.**

2) Name the switch according to the following template: IPF_LAB_<*switch number*>.

3) Delete all ports from the VLAN **default**.

4) For **SW1, SW3** and **SW5:**

Create the VLAN **blue,** give it an IP address in the 10.**N**.0.**N**/24 network, and assign port 1.
Create the VLAN **green,** give it an IP address in the 10.0.0. **N** /24 network, & assign port 5.

For **SW2**, **SW4** and **SW6**:

Create the VLAN **redish,** give it an IP address in the 10.**N**.0. **N** /24 net., & assign port 1.
Create the VLAN **green,** give it an IP address in the 10.0.0. **N** /24 network, & assign port 4.

5) Display the IP route table on the switch using the CLI command **show iproute**

How many routes are in the table? 3

Are there entries for the 10.0.0.0 and 10. **N**.0.0 networks? Yes

What are the metrics for these networks? 1

6) Display the IP configuration for the switch using the CLI command **show ipconfig**

What is the state of IP Routing on the switch? Disabled

7) For **SW1, SW3** and **SW5:**
What is the IP forwarding flag set to for the VLAN's **blue** and **green** ?

For **SW2**, **SW4** and **SW6**:
What is the IP forwarding flag set to for the VLAN's **redish** and **green** ?

S - SubVLAN Proxy

8) Enable IP forwarding for both VLANs on each switch using the CLI command **enable ipforwarding <vlan_name>**.

9) Display the IP configuration for the switch again.

What is the state of IP Routing on the switch this time? Enabled

10) For **SW1, SW3** and **SW5:**
What is the IP forwarding flag set to for the VLAN's **blue** and **green** ?

For **SW2**, **SW4** and **SW6**:
What is the IP forwarding flag set to for the VLAN's **redish** and **green** ?

I - t

Lab13 – IP Forwarding Configuration

11) Configure the laptop with the following parameters:

IP Address = 10.**N**.0.10**N** ; where **N** = Switch Number
IP Mask = 255.255.255.0
Gateway = 10. **N**.0.**N**

12) Using a straight-through CAT5 patch cable, connect the laptop to port 1 on IPF_LAB_ **N**.

Connect port 5 of **SW1, SW3** and/or **SW5:** to port 4 of **SW2, SW4** and/or **SW6** as shown in the network diagram.

13) Display the forwarding database, the ARP table, and the IP forwarding database on the switch using **show fdb**, **show iparp** and **show ipfdb** CLI commands.

How many entries are in the FDB table? a Lot (22)

How many entries are in the ARP table? 1

How many entries are in the IPFDB table? 1

Before proceeding, confirm that your partner switch team on IPF_LAB_N has also completed step (11)

14) From your laptop, ping the **green** vlan interface.

15) Now display the forwarding database, the ARP table, and IP forwarding database on the switch.

How many entries are in the FDB table? 22

How many entries are in the ARP table? 1

Is there an entry for 10.**N**.0.10**N**? Yes

From which VLAN did the switch learn about 10. **N**.0.10**N**? redish

How many entries are in the IPFDB table? 2

16) From your laptop, ping the **green** interface of your partner switch.

Can you reach the far laptop with a ping? No

17) Display the route table on the switch.

Is there an entry for the 10.0.0.0 route? yes

18) From the switch CLI console, ping the **green** interface of your partner switch.

Now can you reach the far switch with a ping? yes

Why can you reach your partner switch from your switch CLI console, but not from your laptop?

Because they are in different Subnets

Lab13 – IP Forwarding Configuration

19) From your laptop, attempt to ping the laptop attached to your partner switch. 10.4.0.104 ~~10.2.0.4~~ 10.30.103

Can you reach the far laptop with a ping? no

20) Display the IP forwarding database on the switch.

Is there an entry for your partner's laptop ipaddress? no

21) Display the route table on the switch.

Is there an entry for your partner switch' network route? no

Why can't you successfully ping the far laptop?

No routing

22) Add a static route for your partner's network 10.**N**.0.0 /24 to the switch route table using 10.0.0.**N** as the gateway and assign this entry a metric of 2 using the CLI command **config iproute add**.

23) Display the route table on the switch.

Is there an entry now for the 10.**N**.0.0 route? yes

What is the origin of this entry? static route

Before proceeding, confirm that your partner switch team on IPF_LAB_N has also completed step (22)

24) From your laptop, attempt to ping the laptop attached to your partner switch.

Can you reach the far laptop with a ping? yes

25) Display the IP forwarding database on the switch.

Is there an entry for your partner's laptop address of 10.**N**.0.10**N**? yes

From which VLAN did the switch learn about 10.**N**.0.10**N**? yes

Before proceeding, confirm that your partner switch team on IPF_LAB_N has also completed step (24)

26) Delete the static route from the switch route table using the CLI command **config iproute delete**.

27) Clear the forwarding database and the IP forwarding database.

28) Display the IP forwarding database.

Is there an entry for your partner's laptop ipaddress 10.**N**.0.10**N**? no

Lab13 – IP Forwarding Configuration

29) Add a default route to the switch route table using your partner's green interface,10.0.0.**N** as the gateway and assign it a metric of 1. Use the CLI command **config iproute add default <ipaddress>**

30) From your laptop, attempt to ping the laptop attached to your partner switch.

Can you reach the far laptop with a ping? yes

31) Display the IP forwarding database on the switch.

Is there an entry for your partner's laptop ipaddress10.**N**.0.10**N**? yes

From which VLAN did the switch learn about ipaddress 10.**N**.0.10**N**? default route

This completes Lab13 – IP Forwarding Configuration Lab.

Lab14 – RIP Configuration

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Setup a network topology for RIP Configuration
2. Configure RIP on the VLAN using the CLI command – **configure rip add vlan** and understand what this command will do.
3. Utilize the CLI commands **enable rip, enable ipforwarding, show ipconfig, show iproute, show rip** and **traceroute <ipaddress>.**

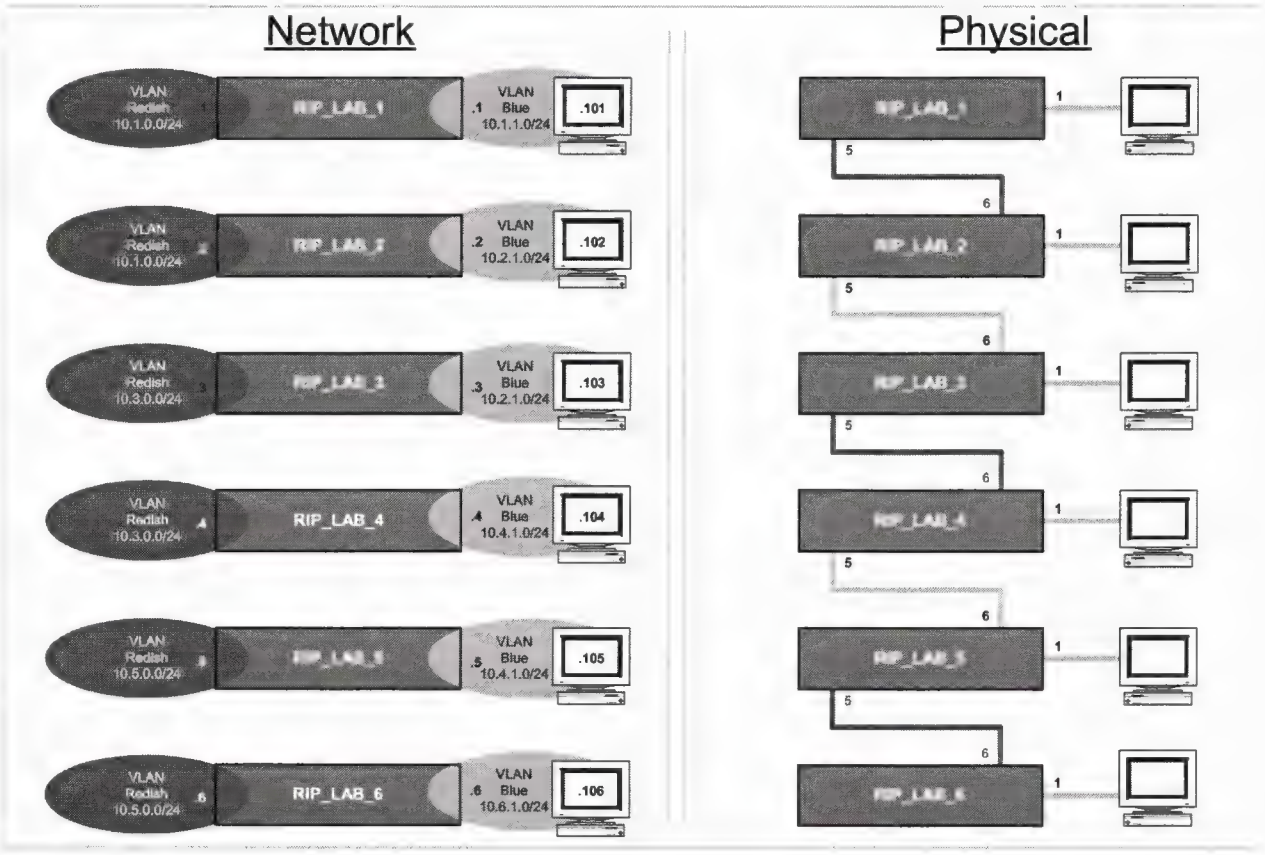
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:



NOTE: Starting with Lab14 through Lab20, ***use the procedure pages that correspond to the switch number of the device you are working on.***

Lab14 – RIP Configuration

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: RIP_LAB_*<switch number>*

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue.**

5) Add port 1 to the VLAN **blue.**

6) Create the VLAN **redish** and assign port 5.

7) Display the IP configuration information for the switch using the **show ipconfig** CLI command.

   What information is displayed for VLANs **redish** and **blue**? _____

   What is missing from the VLAN configuration?

   _____

8) Assign VLAN **blue** an IP address in the 10.1.1.**N**/24 network where N = switch number.

9) Assign VLAN **redish** an IP address in the 10.1.0.**N**/24 network.

10) Display the IP configuration information for the vlans using **show ipconfig vlan** command.

    What is the state of the interface for both VLAN **redish** and VLAN **blue**?

    _____

11) Configure the laptop with the following parameters:

    IP Address = 10.1.1.101
    IP Mask = 255.255.255.0
    Gateway = 10.1.1.1

12) Using a straight-through CAT5 patch cable, connect the laptop to port 1 on RIP_LAB_1.

13) Display the IP configuration for VLAN **blue** only using the CLI command **show ipconfig vlan.**

    What is the state of the interface for VLAN **blue**? _____

14) Display the IP configuration for VLAN **redish** only.

    What is the state of the interface for VLAN **redish**? _____

    Why does VLAN **blue** show as enabled and up while VLAN **redish** still shows as enabled and down?

    _____

15) Using a CAT5 cross-over cable, connect port 5 on RIP_LAB_1 to port 6 on RIP_LAB_2.

Lab14 – RIP Configuration

SW1

16) Display the global IP configuration settings for the switch using the show ipconfig command.

What is the setting for IP routing? _____

17) Enable IP forwarding for VLAN **redish** using the CLI commmand **enable ipforwarding vlan <vlan_name>**.

18) Display the global IP configuration settings again for the switch.

What is the setting for IP routing? _____

19) Display the IP configuration settings for VLAN **redish** only.

What is the setting for IP Forwarding? _____

20) Display the IP configuration settings for VLAN **blue** only.

What is the setting for IP Forwarding? _____

21) Enable IP forwarding for VLAN **blue**

22) Display the IP configuration settings for VLAN **blue** again.

What is the setting for IP Forwarding? _____

23) Display the IP route table for switch RIP_LAB_1 using the CLI command **show iproute**.

How many routes are displayed in the route table? _____

What is the origin of these routes? _____

24) Add VLAN **redish** and VLAN **blue** to the RIP routing protocol using the CLI command **configure rip add vlan <vlan_name>.**

25) Display the IP configuration information for VLAN **redish** and VLAN **blue**

What is the setting for RIP on vlan **redish**? _____

What is the setting for RIP on vlan **blue**? _____

What is the purpose of adding a VLAN to the routing protocol?

_____

_____

_____

26) Enable the RIP routing protocol on the switch using the CLI command **enable rip**.

27) Display the global IPC switch settings for RIP_LAB_1.

What is the setting for RIP on switch RIP_LAB_1? _____

_____

Lab14 – RIP Configuration

Before proceeding, confirm that all of the other teams have also enabled RIP on their switches.

28) Display the IP route table for switch RIP_LAB_1.

How many routes are displayed in the route table? _____

What is the origin of these routes?

_____

29) Open a DOS window on the laptop and ping all of the other laptops in the network:

How many laptops respond to the ping?

_____

30) From the same DOS window, perform a traceroute to the laptop connected to RIP_LAB_6. tracert 10.6.1.106.

How many hops does it take the traceroute to reach the destination IP address?

_____

This completes Lab 14 – RIP Configuration I – Switch 1

Lab14 – RIP Configuration I

SW2

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: RIP_LAB_<*switch number*>

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue.**

5) Assign port 1 and 5 to VLAN **blue**.

6) Create the VLAN **redish** and assign port 6.

7) Display the IP configuration information for the switch using the **show ipconfig** CLI command.

   What information is displayed for VLANs **redish** and **blue**? _____

   What is missing from the VLAN configuration?

   _____

8) Assign VLAN **blue** an IP address in the 10.2.1.**N**/24 network.

9) Assign VLAN **redish** an IP address in the 10.1.0.**N**/24 network.

10) Display the IP configuration information for the vlans using **show ipconfig vlan** command.

    What is the state of the interface for both VLAN **redish** and VLAN **blue**?

    _____

11) Configure the laptop with the following parameters:

    IP Address = 10.2.1.102
    IP Mask = 255.255.255.0
    Gateway = 10.2.1.2

12) Using a straight-through CAT5 patch cable, connect the laptop to port 1 on RIP_LAB_2.

13) Display the IP configuration for VLAN **blue** only using the CLI command **show ipconfig vlan**.

    What is the state of the interface for VLAN **blue**? _____

14) Display the IP configuration for VLAN **redish** only.

    What is the state of the interface for VLAN **redish**? _____

    Why does VLAN **blue** show as enabled and up while VLAN **redish** still shows as enabled and down?

    _____

15) Using a CAT5 cross-over cable, connect port 6 on RIP_LAB_2 to port 5 on RIP_LAB_1 and port 5 on RIP_LAB_2 to port 6 on RIP_LAB_3.

_____

Lab14 – RIP Configuration I

16) Display the global IP configuration settings for the switch.

What is the setting for IP routing? _____

17) Enable IP forwarding for VLAN **redish** using the CLI command **enable ipforwarding vlan <vlan_name>.**

18) Display the global IP configuration settings again for the switch.

What is the setting for IP routing? _____

19) Display the IP configuration settings for VLAN **redish** only.

What is the setting for IP Forwarding? _____

20) Display the IP configuration settings for VLAN **blue** only.

What is the setting for IP Forwarding? _____

21) Enable IP forwarding for VLAN **blue**

22) Display the IP configuration settings for VLAN **blue** again.

What is the setting for IP Forwarding? _____

23) Display the IP route table for switch RIP_LAB_2 using the CLI command **show iproute**.

How many routes are displayed in the route table? _____

What is the origin of these routes? _____

Every switch has an entry for the network 127.0.0.1. What is the significance of this entry?

_____

24) Add VLAN **redish** and VLAN **blue** to the RIP routing protocol using the CLI command **configure rip add vlan <vlan_name>.**

25) Display the IP configuration information for VLAN **redish** and VLAN **blue**

What is the setting for RIP on vlan **redish**? _____

What is the setting for RIP on vlan **blue**? _____

What is the purpose of adding a VLAN to the routing protocol?

_____

_____

_____

Will a VLAN so configured begin the RIP update process immediately?

_____

_____

Lab14 – RIP Configuration I

SW2

26) Enable the RIP routing protocol on the switch using the CLI command **enable rip**.

27) Display the global IPC switch settings for RIP_LAB_2.

What is the setting for RIP on switch RIP_LAB_2? _____

What is the purpose of enabling RIP on the switch?

_____

_____

Before proceeding, confirm that all of the other teams have also enabled RIP on their switches.

28) Display the IP route table for switch RIP_LAB_2

How many routes are displayed in the route table? _____

What is the origin of these routes?

_____

29) Open a DOS window on the laptop and ping all of the other laptops in the network:

How many laptops respond to the ping?

_____

30) From the same DOS window, perform a traceroute to the laptop connected to RIP_LAB_6. tracert 10.6.1.106

How many hops does it take the traceroute to reach the destination IP address?

_____

If RIP_LAB_2 is one switch further from RIP_LAB_6 as RIP_LAB_3, why does the laptop on RIP_LAB_2 take the same number of hops to reach 10.6.1.106 as the laptop on RIP_LAB_3?

_____

_____

This completes Lab 14 RIP Configuration I – Switch 2

_____

Lab14 – RIP Configuration I

SW3

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: RIP_LAB_<*switch number*>

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue.**

5) Assign port 1 and 6 to VLAN **blue**.

6) Create the VLAN **redish** and assign port 5.

7) Display the IP configuration information for the switch using the **show ipconfig** CLI command.

   What information is displayed for VLANs redish and **blue**? _____

   What is missing from the VLAN configuration?

   _____

8) Assign VLAN **blue** an IP address in the 10.2.1.**N**/24 network.

9) Assign VLAN **redish** an IP address in the 10.3.0.**N**/24 network.

10) Display the IP configuration information for the vlans using **show ipconfig vlan** command.

    What is the state of the interface for both VLAN redish and VLAN **blue**?

    _____

11) Configure the laptop with the following parameters:

    IP Address = 10.2.1.103
    IP Mask = 255.255.255.0
    Gateway = 10.2.1.3

    Looking at the network diagram, could any other interface in the network be used for the gateway address?

    _____

12) Using a straight-through CAT5 patch cable, connect the laptop to port 1 on RIP_LAB_3.

13) Display the IP configuration for VLAN **blue** only using the CLI command **show ipconfig vlan**.

    What is the state of the interface for VLAN **blue**? _____

14) Display the IP configuration for VLAN **redish** only.

    What is the state of the interface for VLAN **redish**? _____
    Why does VLAN **blue** show as enabled and up while VLAN **redish** still shows as enabled and down?

    _____

_____

Lab14 – RIP Configuration I

15) Using a CAT5 cross-over cable, connect port 6 on RIP_LAB_3 to port 5 on RIP_LAB_2 and port 5 on RIP_LAB_3 to port 6 on RIP_LAB_4.

16) Display the global IP configuration settings for the switch.

What is the setting for IP routing? _____

17) Enable IP forwarding for VLAN redish using the CLI command **enable ipforwarding vlan <vlan_name>.**

18) Display the global IP configuration settings again for the switch.

What is the setting for IP routing? _____

19) Display the IP configuration settings for VLAN **redish** only.

What is the setting for IP Forwarding? _____

20) Display the IP configuration settings for VLAN **blue** only.

What is the setting for IP Forwarding? _____

21) Enable IP forwarding for VLAN **blue**

22) Display the IP configuration settings for VLAN **blue** again.

What is the setting for IP Forwarding? _____

23) Display the IP route table for switch RIP_LAB_3 using the CLI command **show iproute**.

How many routes are displayed in the route table? _____

What is the origin of these routes? _____

Every switch has an entry for the network 127.0.0.1. What is the significance of this entry?

_____

24) Add VLAN **redish** and VLAN **blue** to the RIP routing protocol using the CLI command **configure rip add vlan <vlan_name>.**

25) Display the IP configuration information for VLAN redish and VLAN **blue**

What is the setting for RIP on vlan **redish**? _____

What is the setting for RIP on vlan **blue**? _____

What is the purpose of adding a VLAN to the routing protocol?

_____

_____

_____

_____

Will a VLAN so configured begin the RIP update process immediately?

_____

26) Enable the RIP routing protocol on the switch using the CLI command **enable rip**.

27) Display the global IPC switch settings for RIP_LAB_3.

What is the setting for RIP on switch RIP_LAB_3? _____

What is the purpose of enabling RIP on the switch?

_____

_____

Before proceeding, confirm that all of the other teams have also enabled RIP on their switches.

28) Display the IP route table for switch RIP_LAB_3

How many routes are displayed in the route table? _____

What is the origin of these routes?

_____

29) Open a DOS window on the laptop and ping all of the other laptops in the network:

How many laptops respond to the ping?

_____

30) From the same DOS window, perform a traceroute to the laptop connected to RIP_LAB_6.
tracert 10.6.1.106

How many hops does it take the traceroute to reach the destination IP address?

_____

If RIP_LAB_3 is one switch closer to RIP_LAB_6 than RIP_LAB_2, why does the laptop on RIP_LAB_3 take the same number of hops to reach 10.6.1.106 as the laptop on RIP_LAB_2?

_____

_____

This completes Lab14 – RIP Configuration I – Switch 3

_____

Lab14 – RIP Configuration I

SW4

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: RIP_LAB_<*switch number*>

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue.**

5) Assign port 1 and 5 to VLAN **blue**.

6) Create the VLAN **redish** and assign port 6.

7) Display the IP configuration information for the switch using the **show ipconfig** CLI command.

   What information is displayed for VLANs **redish** and **blue**? no infor for redish/blue

   What is missing from the VLAN configuration?

   no route

8) Assign VLAN **blue** an IP address in the 10.4.1.**N**/24 network.

9) Assign VLAN **redish** an IP address in the 10.3.0.**N**/24 network.

10) Display the IP configuration information for the vlans using **show ipconfig vlan** command.

    What is the state of the interface for both VLAN **redish** and VLAN **blue**?

    Blue (up), redish (down), Both are enabled

11) Configure the laptop with the following parameters:

    IP Address = 10.4.1.104
    IP Mask = 255.255.255.0
    Gateway = 10.4.1.4

    Looking at the network diagram, could any other interface in the network be used for the gateway address?

    10.3.0.4 (on VLAN redish)

12) Using a straight-through CAT5 patch cable, connect the laptop to port 1 on RIP_LAB_4.

13) Display the IP configuration for VLAN **blue** only using the CLI command **show ipconfig vlan**.

    What is the state of the interface for VLAN **blue**? up

14) Display the IP configuration for VLAN **redish** only.

    What is the state of the interface for VLAN **redish**? down
    Why does VLAN **blue** show as enabled and up while VLAN **redish** still shows as enabled and down?

    My workstation is on the same subnet as Blue but different subnet as redish

Lab14 – RIP Configuration I

15) Using a CAT5 cross-over cable, connect port 6 on RIP_LAB_4 to port 5 on RIP_LAB_3 and port 5 on RIP_LAB_4 to port 6 on RIP_LAB_5.

16) Display the global IP configuration settings for the switch.

What is the setting for IP routing? Disabled

17) Enable IP forwarding for VLAN **redish** using the CLI command **enable ipforwarding vlan <vlan_name>.**

18) Display the global IP configuration settings again for the switch.

What is the setting for IP routing? enabled

19) Display the IP configuration settings for VLAN **redish** only.

What is the setting for IP Forwarding? yes

20) Display the IP configuration settings for VLAN **blue** only.

What is the setting for IP Forwarding? no

21) Enable IP forwarding for VLAN **blue**

22) Display the IP configuration settings for VLAN **blue** again.

What is the setting for IP Forwarding? yes

23) Display the IP route table for switch RIP_LAB_4 using the CLI command **show iproute**.

How many routes are displayed in the route table? 3

What is the origin of these routes? _____

Every switch has an entry for the network 127.0.0.1. What is the significance of this entry?

loopbackroute, route are not in the routing table
Will be sent to Default Route

24) Add VLAN **redish** and VLAN **blue** to the RIP routing protocol using the CLI command **configure rip add vlan <vlan_name>.**

25) Display the IP configuration information for VLAN **redish** and VLAN **blue**

What is the setting for RIP on vlan **redish**? yes

What is the setting for RIP on vlan **blue**? yes

What is the purpose of adding a VLAN to the routing protocol?

Traffic on VLAN on different vlans will be transmitted to Destination on different subnets

Lab14 – RIP Configuration I

SW4

Will a VLAN so configured begin the RIP update process immediately?

26) Enable the RIP routing protocol on the switch using the CLI command **enable rip**.

27) Display the global IPC switch settings for RIP_LAB_4.

What is the setting for RIP on switch RIP_LAB_4? enabled

What is the purpose of enabling RIP on the switch?

Route to the diffrent Subnets

Before proceeding, confirm that all of the other teams have also enabled RIP on their switches.

28) Display the IP route table for switch RIP_LAB_4

How many routes are displayed in the route table? 8

What is the origin of these routes?

10.4.1.0 127.0.0.1

10.3.0.0

29) Open a DOS window on the laptop and ping all of the other laptops in the network:

How many laptops respond to the ping?

30) From the same DOS window, perform a traceroute to the laptop connected to RIP_LAB_1. tracert 10.1.1.101

How many hops does it take the traceroute to reach the destination IP address?

5 hops

If RIP_LAB_4 is one switch closer to RIP_LAB_1 than RIP_LAB_5, why does the laptop on RIP_LAB_5 take the same number of hops to reach 10.1.1.101 as the laptop on RIP_LAB_4?

Lab 4 and 5 are on the same subnets

This completes Lab14 – RIP Configuration I – Switch 4

Lab14 – RIP Configuration I

SW5

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: RIP_LAB_<*switch number*>

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue.**

5) Assign port 1 and 6 to VLAN **blue**.

6) Create the VLAN **redish** and assign port 5.

7) Display the IP configuration information for the switch using the **show ipconfig** CLI command.

   What information is displayed for VLANs **redish** and **blue**? _____

   What is missing from the VLAN configuration?

   _____

8) Assign VLAN **blue** an IP address in the 10.4.1.**N**24 network.

9) Assign VLAN **redish** an IP address in the 10.5.0.**N**/24 network.

10) Display the IP configuration information for the vlans using **show ipconfig vlan** command.

    What is the state of the interface for both VLAN **redish** and VLAN **blue**?

    _____

11) Configure the laptop with the following parameters:

    IP Address = 10.4.1.105
    IP Mask = 255.255.255.0
    Gateway = 10.4.1.5

    Looking at the network diagram, could any other interface in the network be used for the gateway address?

    _____

12) Using a straight-through CAT5 patch cable, connect the laptop to port 1 on RIP_LAB_5.

13) Display the IP configuration for VLAN **blue** only using the CLI command **show ipconfig vlan**.

    What is the state of the interface for VLAN **blue**? _____

14) Display the IP configuration for VLAN **redish** only.

    What is the state of the interface for VLAN **redish**? _____
    Why does VLAN **blue** show as enabled and up while VLAN **redish** still shows as enabled and down?

    _____

_____

Lab14 – RIP Configuration I

15) Using a CAT5 cross-over cable, connect port 6 on RIP_LAB_5 to port 5 on RIP_LAB_4 and port 5 on RIP_LAB_5 to port 6 on RIP_LAB_6.

16) Display the global IP configuration settings for the switch.

What is the setting for IP routing? _____

17) Enable IP forwarding for VLAN **redish** using the CLI command **enable ipforwarding vlan <vlan_name>.**

18) Display the global IP configuration settings again for the switch.

What is the setting for IP routing? _____

19) Display the IP configuration settings for VLAN **redish** only.

What is the setting for IP Forwarding? _____

20) Display the IP configuration settings for VLAN **blue** only.

What is the setting for IP Forwarding? _____

21) Enable IP forwarding for VLAN **blue**

22) Display the IP configuration settings for VLAN **blue** again.

What is the setting for IP Forwarding? _____

23) Display the IP route table for switch RIP_LAB_5 using the CLI command **show iproute**.

How many routes are displayed in the route table? _____

What is the origin of these routes? _____

Every switch has an entry for the network 127.0.0.1. What is the significance of this entry?

_____

24) Add VLAN **redish** and VLAN **blue** to the RIP routing protocol using the CLI command **configure rip add vlan <vlan_name>.**

25) Display the IP configuration information for VLAN **redish** and VLAN **blue**

What is the setting for RIP on vlan **redish**? _____

What is the setting for RIP on vlan **blue**? _____

What is the purpose of adding a VLAN to the routing protocol?

_____

_____

_____

_____

Will a VLAN so configured begin the RIP update process immediately?

_____

26) Enable the RIP routing protocol on the switch using the CLI command **enable rip**.

27) Display the global IPC switch settings for RIP_LAB_5.

What is the setting for RIP on switch RIP_LAB_5? _____

What is the purpose of enabling RIP on the switch?

_____

_____

Before proceeding, confirm that all of the other teams have also enabled RIP on their switches.

28) Display the IP route table for switch RIP_LAB_5.

How many routes are displayed in the route table? _____

What is the origin of these routes?

_____

29) Open a DOS window on the laptop and ping all of the other laptops in the network:

How many laptops respond to the ping?

_____

30) From the same DOS window, perform a traceroute to the laptop connected to RIP_LAB_1. tracert 10.1.1.101

How many hops does it take the traceroute to reach the destination IP address?

_____

If RIP_LAB_5 is one switch further from RIP_LAB_1 than RIP_LAB_4, why does the laptop on RIP_LAB_5 take the same number of hops to reach 10.1.1.101 as the laptop on RIP_LAB_4?

_____

_____

This completes Lab14 – RIP Configuration I – Switch 5

_____

Lab14 – RIP Configuration I

SW6

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: RIP_LAB_<*switch number*>

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue.**

5) Assign port 1 to the VLAN **blue.**

6) Create the VLAN **redish** and assign port 6.

7) Display the IP configuration information for the switch using the **show ipconfig** CLI command.

   What information is displayed for VLANs **redish** and **blue**? _____

   What is missing from the VLAN configuration?

   _____

8) Assign VLAN **blue** an IP address in the 10.6.1.**N**/24 network.

9) Assign VLAN **redish** an IP address in the 10.5.0.**N**/24 network.

10) Display the IP configuration information for the vlans using **show ipconfig vlan** command.

    What is the state of the interface for both VLAN **redish** and VLAN **blue**?

    _____

11) Configure the laptop with the following parameters:

    IP Address = 10.6.1.106
    IP Mask = 255.255.255.0
    Gateway = 10.6.1.6

12) Using a straight-through CAT5 patch cable, connect the laptop to port 1 on RIP_LAB_6.

13) Display the IP configuration for VLAN **blue** only using the CLI command **show ipconfig vlan.**

    What is the state of the interface for VLAN **blue**? _____

14) Display the IP configuration for VLAN **redish** only.

    What is the state of the interface for VLAN **redish**? _____

    Why does VLAN **blue** show as enabled and up while VLAN **redish** still shows as enabled and down?

    _____

15) Using a CAT5 cross-over cable, connect port 36 on RIP_LAB_6 to port 25 on RIP_LAB_5.

_____

Lab14 – RIP Configuration I

16) Display the global IP configuration settings for the switch using the show ipconfig command.

What is the setting for IP routing? _____

17) Enable IP forwarding for VLAN **redish** using the CLI commmand **enable ipforwarding vlan <vlan_name>**.

18) Display the global IP configuration settings again for the switch.

What is the setting for IP routing? _____

19) Display the IP configuration settings for VLAN **redish** only.

What is the setting for IP Forwarding? _____

20) Display the IP configuration settings for VLAN **blue** only.

What is the setting for IP Forwarding? _____

21) Enable IP forwarding for VLAN **blue**

22) Display the IP configuration settings for VLAN **blue** again.

What is the setting for IP Forwarding? _____

23) Display the IP route table for switch RIP_LAB_6 using the CLI command **show iproute**.

How many routes are displayed in the route table? _____

What is the origin of these routes? _____

Every switch has an entry for the network 127.0.0.1. What is the significance of this entry?

_____

24) Add VLAN **redish** and VLAN **blue** to the RIP routing protocol using the CLI command **configure rip add vlan <vlan_name>.**

25) Display the IP configuration information for VLAN **redish** and VLAN **blue**

What is the setting for RIP on vlan **redish**? _____

What is the setting for RIP on vlan **blue**? _____

What is the purpose of adding a VLAN to the routing protocol?

_____

_____

_____

Will a VLAN so configured begin the RIP update process immediately?

_____

Lab14 – RIP Configuration I

SW6

26) Enable the RIP routing protocol on the switch using the CLI command **enable rip**.

27) Display the global IPC switch settings for RIP_LAB_6.

What is the setting for RIP on switch RIP_LAB_6? _____

What is the purpose of enabling RIP on the switch?

_____

_____

Before proceeding, confirm that all of the other teams have also enabled RIP on their switches.

28) Display the IP route table for switch RIP_LAB_6.

How many routes are displayed in the route table? _____

What is the origin of these routes?

_____

29) Open a DOS window on the laptop and ping all of the other laptops in the network:

How many laptops respond to the ping?

_____

30) From the same DOS window, perform a traceroute to the laptop connected to RIP_LAB_1. tracert 10.1.1.101.

How many hops does it take the traceroute to reach the destination IP address?

_____

This completes Lab14 – RIP Configuration I – Switch 6

_____

Lab15 – OSPF Configuration I

SW1

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Setup and configure a network with the topology provided. Create VLANs as shown.
2. Create an OSPF area and add a VLAN to it using the CLI command: **create ospf area, config ospf add.**
3. Determine what is required for routing to work and what to enable for OSPF to work on a VLAN.
4. Display the area information using the CLI command: **sh ospf area all.**
5. Configure the laptop and add it to the configured network running OSPF and verify via PING if the connection works.

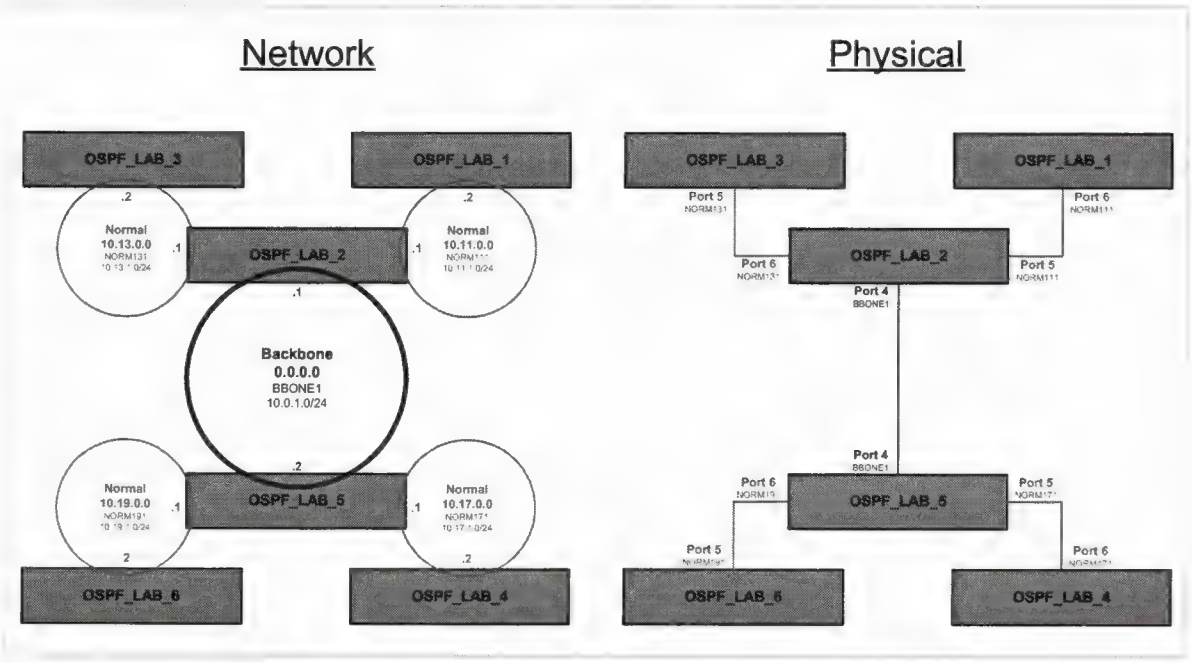
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: *Switch Station 1*



1) Clear the switch of all old configuration information. Then Logon as admin.

2) Name the switch according to the following template: OSPF1_LAB_<*switch number*>

3) Delete all ports out of the default VLAN **default**.

Lab15 – OSPF Configuration I

4) Create the VLAN **norm111**, give it an IP address in the 10.11.1.**0**/24 network using the convention shown in the diagram. Assign ports 1 & 6 (port 1 will be used to connect the PC-laptop).

5) Create the OSPF area **10.11.0.0** using the CLI command: **create ospf area.**

6) Display the IP configuration statistics for the VLAN **norm111**.

   What two flags must be set to YES for OSPF to work on this VLAN?

   _____

7) Enable the VLAN **norm111** for OSPF by adding it to area **10.11.0.0** using the CLI command **config ospf add vlan_name area <area_id>**.

   What warning message did you get when the command was executed?

   _____

   What do you need to do before routing will work?

   _____

8) Enable IP forwarding for the VLAN **norm111**.

9) What command displays the state of the OSPF routing protocol? _____

   Enable the OSPF routing protocol for the switch.

10) Save the newly-created switch configuration to the secondary file location.

11) Display the OSPF area information.

   How many areas are configured on the switch? _____

   How many interfaces are in the area 10.11.0.0? _____

   What is the state of the interface(s) in area 10.11.0.0 and what does it stand for?

   _____

12) Connect port 6 on switch OSPF_LAB_1 to port 5 on switch OSPF_LAB_2.

13) Once all the switches are cabled together, display the OSPF information for the VLAN **norm111** using the CLI command **show ospf interface <vlan_name>**

   What is the router ID for the Designated Router? _____

   What is the IP Address for the Designated Router?_____

   Is the ID and the IP address for the Designated Router different or the same? Why is it?

   _____

   _____

Lab15 – OSPF Configuration I

SW1

What is the state of the neighbor connection? _____

13) Display the area information for 10.11.0.0

What is the state of the interface in the area 10.11.0.0 and what does it mean?

_____

14) Configure the laptop with the following parameters:

IP Address = 10.11.1.201
IP Mask = 255.255.255.0
Gateway = 10.11.1.2

16) Connect the laptop to Port 1 on switch OSPF_LAB_1.

17) Ping the gateway interface from the laptop.

Is the ping successful? _____

18) Ping the interface 10.13.1.2 from the laptop.

Is the ping successful? _____

19) Change the laptop gateway to 10.11.1.1.

20) Ping the interface 10.13.1.2 from the laptop.

Is the ping successful? _____

This completes Lab 15 – OSPF Configuration I – Switch 1

Lab15 – OSPF Configuration I

SW2

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Setup and configure a network with the topology provided. Create VLANs as shown.
2. Create an OSPF area and add a VLAN to it using the CLI command: **create ospf area, config ospf add** and other commands.
3. Determine what is required for routing to work and what to enable for OSPF to work on a VLAN.
4. Display the area information using the CLI command: **sh ospf area all.**
5. Configure the laptop and add it to the configured network running OSPF and verify via PING if the connection works.

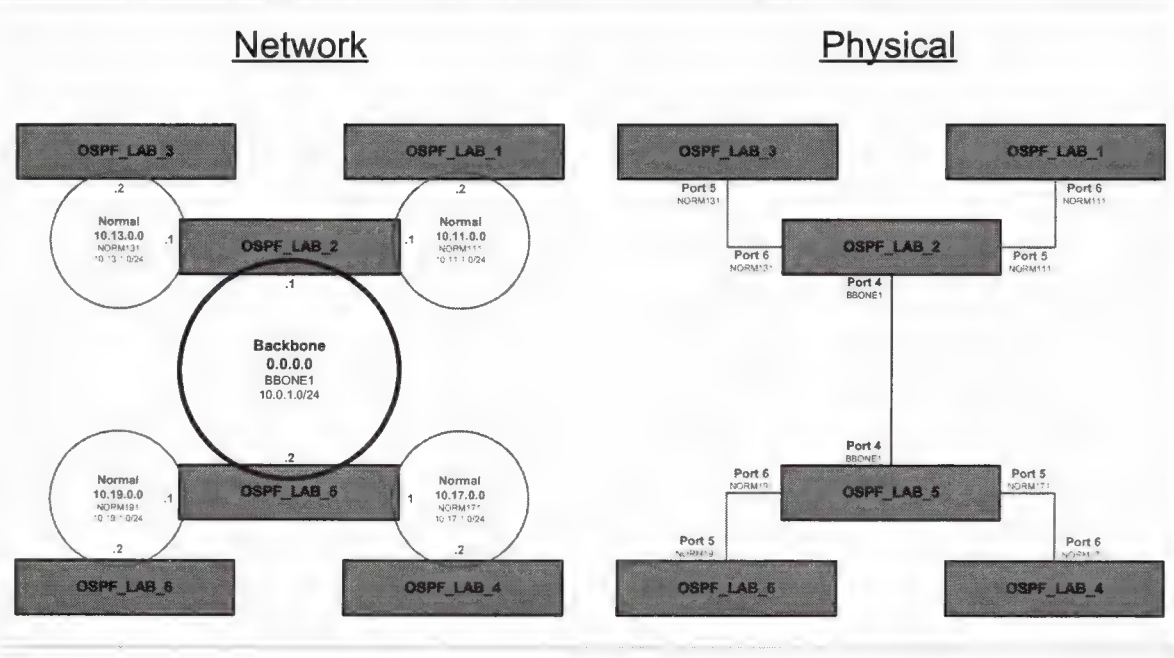
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: *Switch Station 2*



1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: OSPF_LAB_<switch number>

3) Delete all ports out of the default VLAN **default**.

Lab15 – OSPF Configuration I

4) Create the VLAN **norm111**, give it an IP address in the 10.11.1.**0**/24 network using the convention shown in the diagram. Assign port 5 untagged.

5) Create the VLAN **norm131**, give it an IP address in the 10.13.1.**0**/24 network using the convention shown in the diagram. Assign port 6 untagged.

6) Create the VLAN **bbone1**, give it an IP address in the 10.0.1.**0**/24 network, using the convention shown in the diagram. Assign ports 1 and 4, untagged (port 1 will be used to connect the workstation).

7) Create the OSPF area **10.11.0.0** and area **10.13.0.0** using the CLI command: **create ospf area.**

8) Display the IP configuration statistics for the VLAN **norm111**.

   What two flags must be set to YES for OSPF to work on this VLAN?

   _____

9) Enable the VLANs **norm111**, **norm131**, and **bbone1** for OSPF by adding it to area **10.11.0.0,** area **10.13.0.0,** and area **0.0.0.0** respectively using the CLI command **config ospf add vlan_name area <area_id>**..

   What warning message do you get when you add the VLAN to the OSPF area?

   _____

   What do you need to do before routing will work?

   _____

10) Enable IP forwarding for the VLAN **norm111**, **norm131**, and **bbone1**.

11) What command displays the state of the OSPF routing protocol? _____

12) Enable the OSPF routing protocol for the switch.

13) Save the newly created switch configuration to the secondary file location.

14) Display the OSPF area information.

    How many areas are configured on the switch? _____

    How many interfaces are in the area 10.11.0.0? _____

    What is the state of the interface(s) in area 0.0.0.0 and what does it stand for?

    _____

15) Connect port 6 on switch OSPF_LAB_2 to port 5 on switch OSPF_LAB_3, port 5 on switch OSPF_LAB_2 to port 6 on OSPF_LAB_1, and port 4 on OSPF_LAB_2 to port 4 on OSPF_LAB_5.

16) Once all the switches are cabled together, display the OSPF information for the VLAN **norm111** using the CLI command **show ospf interface <vlan_name>**

_____

Lab15 – OSPF Configuration I

SW2

What is the router ID for the Designated Router? _____

What is the IP Address for the Designated Router?_____

Is the ID and the IP address for the Designated Router different or the same? Why is it?

_____

_____

What is the state of the neighbor connection? _____

17) Display the area information for 10.11.0.0

What is the state of the interface in the area 10.11.0.0 and what does it mean?

_____

18) Configure the laptop with the following parameters:

IP Address = 10.0.1.201
IP Mask = 255.255.255.0
Gateway = 10.0.1.1

19) Connect the laptop to Port 1 on switch OSPF_LAB_2.

20) Ping the gateway interface from the laptop.

Is the ping successful? _____

21) Ping the interfaces 10.17.1.2 and 10.19.1.2. Is the ping successful?_____

This completes Lab 15 – OSPF Configuration I – Switch 2

Lab15 – OSPF Configuration I

SW3

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Setup and configure a network with the topology provided. Create VLANs as shown.
2. Create an OSPF area and add a VLAN to it using the CLI command: **create ospf area, config ospf add.**
3. Determine what is required for routing to work and what to enable for OSPF to work on a VLAN.
4. Display the area information using the CLI command: **sh ospf area all.**
5. Configure the laptop and add it to the configured network running OSPF and verify via PING if the connection works.

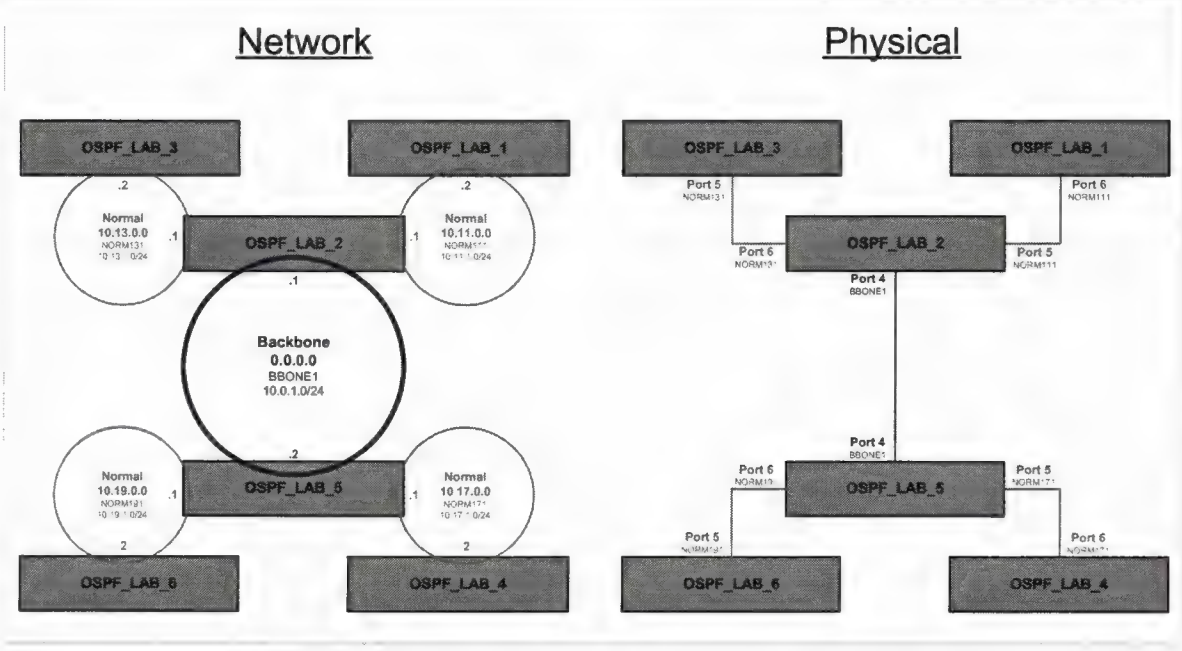
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: *Switch Station 3*



1) Clear the switch of all old configuration information. Then Logon as admin.

2) Name the switch according to the following template: OSPF_LAB_<*switch number*>

3) Delete all ports out of the default VLAN **default**.

Lab15 – OSPF Configuration I

4) Create the VLAN **norm131**, give it an IP address in the 10.13.1.**0**/24 network, using the convention shown in the diagram. Assign ports 1 and 5 (port 1 will be used to connect the workstation).

5) Create the OSPF area 10.13.0.0 using the CLI command: **create ospf area**.

6) Display the IP configuration statistics for the VLAN **norm131**.

   What two flags must be set to YES for OSPF to work on this VLAN?

   _____

7) Enable the VLAN **norm131** for OSPF by adding it to area 10.13.0.0 using the CLI command: **config ospf add vlan_name area <area_id>.**

   What warning message do you get when you add the VLAN to the OSPF area?

   _____

   What do you need to do before routing will work?

   _____

8) Enable IP forwarding for the VLAN **norm131**.

9) What command displays the state of the OSPF routing protocol? _____

   Enable the OSPF routing protocol for the switch.

10) Save the newly-created switch configuration to the secondary file location.

11) Display the OSPF area information.

    How many areas are configured on the switch? _____

    How many interfaces are in the area 10.13.0.0? _____

    What is the state of the interface(s) in area 10.13.0.0 and what does it stand for?

    _____

12) Connect port 5 on switch OSPF_LAB_3 to port 6 on switch OSPF_LAB_2.

13) Once all the switches are cabled together display the OSPF information for the VLAN **norm131** using the CLI command **show ospf interface <vlan_name>**

    What is the router ID for the Designated Router? _____

    What is the IP Address for the Designated Router?_____

    Is the ID and the IP address for the Designated Router different or the same? Why is it?

    _____

    _____

Lab15 – OSPF Configuration I

SW3

What is the state of the neighbor connection? _____

14) Display the area information for 10.13.0.0

What is the state of the interface in the area 10.13.0.0 and what does it mean?

_____

15) Configure the laptop with the following parameters:

IP Address = 10.13.1.201
IP Mask = 255.255.255.0
Gateway = 10.13.1.2

16) Connect the laptop to Port 1 on switch OSPF_LAB_3.

17) Ping the gateway interface from the laptop.

Is the ping successful? _____

18) Ping the interface 10.11.1.2 from the laptop.

Is the ping successful? _____

19) Change the laptop gateway to 10.13.1.1.

20) Ping the interface 10.11.1.2 from the laptop.

Is the ping successful? _____

This completes La15 – OSPF Configuration I – Switch 3

_____

Lab15 – OSPF Configuration I

SW4

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Setup and configure a network with the topology provided. Create VLANs as shown.
2. Create an OSPF area and add a VLAN to it using the CLI command: **create ospf area, config ospf add.**
3. Determine what is required for routing to work and what to enable for OSPF to work on a VLAN.
4. Display the area information using the CLI command: **sh ospf area all.**
5. Configure the laptop and add it to the configured network running OSPF and verify via PING if the connection works.

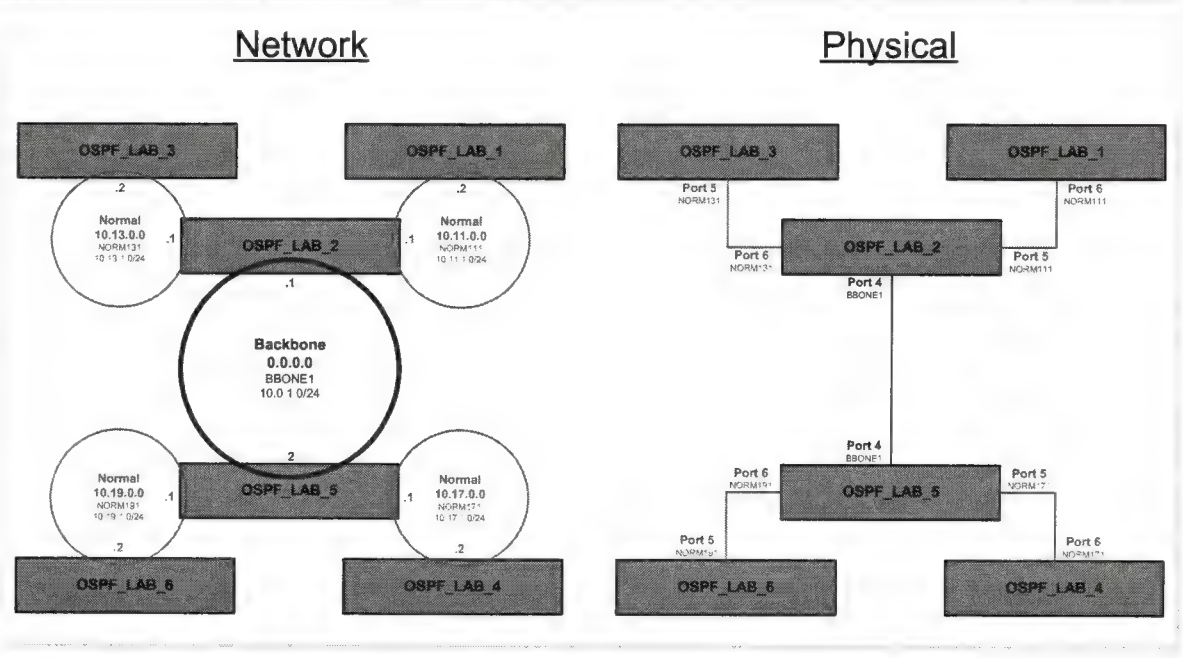
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: *Switch Station 4*



1) Clear the switch of all old configuration information. Then Logon as admin.

2) Name the switch according to the following template: OSPF_LAB_*<switch number>*

3) Delete all ports out of the default VLAN **default**.

Lab15 – OSPF Configuration I

4) Create the VLAN **norm171**, give it an IP address in the 10.17.1.0/24 network, using the convention shown in the diagram. Assign ports 1 and 6 (port 1 will be used to connect the workstation).

5) Create the OSPF area **10.17.0.0** using the CLI command: **create ospf area**.

6) Display the IP configuration statistics for the VLAN **norm171**.

What two flags must be set to YES for OSPF to work on this VLAN?

OSPF, IP forwarding

7) Enable the VLAN **norm171** for OSPF by adding it to area 10.17.0.0 using the CLI command: **config ospf add vlan_name area <area_id>.**

What warning message do you get when you add the VLAN to the OSPF area?

✓ area 10.17.0.0 doesn't exist

What do you need to do before routing will work? enable OSPF

(~~create OSPF area 10.17.0.0~~)

8) Enable IP forwarding for the VLAN **norm171**.

9) What command displays the state of the OSPF routing protocol? show OSPF

Enable the OSPF routing protocol for the switch.

10) Save the newly created switch configuration to the secondary file location.

11) Display the OSPF area information.

How many areas are configured on the switch? 2 area (0.0.0.0) (10.17.0.0)

How many interfaces are in the area 10.17.0.0? 1

What is the state of the interface(s) in area 10.17.0.0 and what does it stand for?

Down - interface

12) Connect port 6 on switch OSPF_LAB_4 to port 5 on switch OSPF_LAB_5.

13) Once all the switches are cabled together, display the OSPF information for the VLAN **norm171** using the CLI command **show ospf interface <vlan_name>**

What is the router ID for the Designated Router? 0.0.0.0

What is the IP Address for the Designated Router? 0.0.0.0

Is the ID and the IP address for the Designated Router different or the same? Why is it?

Same

Lab15 – OSPF Configuration I

SW4

What is the state of the neighbor connection? N/A

14) Display the area information for 10.17.0.0

What is the state of the interface in the area 10.17.0.0 and what does it mean?

15) Configure the laptop with the following parameters:

IP Address = 10.17.1.201
IP Mask = 255.255.255.0
Gateway = 10.17.1.2

16) Connect the laptop to Port 1 on switch OSPF_LAB_4.

17) Ping the gateway interface from the laptop.

Is the ping successful? yes

18) Ping the interface 10.19.1.2 from the laptop.

Is the ping successful? yes

19) Change the laptop gateway to 10.17.1.1.

20) Ping the interface 10.19.1.2 from the laptop.

Is the ping successful? yes

This completes Lab 15 – OSPF Configuration I – Switch 4

Lab15 – OSPF Configuration I

SW5

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Setup and configure a network with the topology provided. Create VLANs as shown.
2. Create an OSPF area and add a VLAN to it using the CLI command: **create ospf area, config ospf add** and other commands.
3. Determine what is required for routing to work and what to enable for OSPF to work on a VLAN.
4. Display the area information using the CLI command: **sh ospf area all.**
5. Configure the laptop and add it to the configured network running OSPF and verify via PING if the connection works.

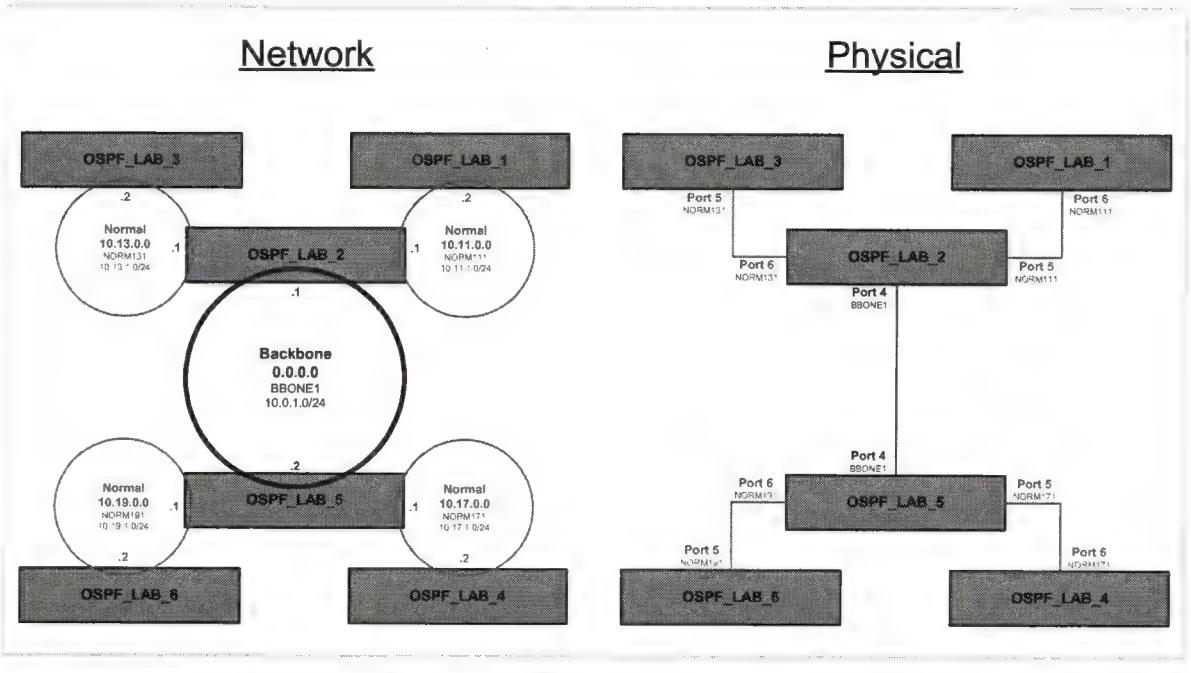
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: *Switch Station 5*



1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: OSPF_LAB_<switch number>

3) Delete all ports out of the default VLAN **default**.

Lab15 – OSPF Configuration I

4) Create the VLAN **norm171**, give it an IP address in the 10.17.1.**0**/24 network, using the convention shown in the diagram. Assign port 5 untagged.

5) Create the VLAN **norm191**, give it an IP address in the 10.19.1.**0**/24 network, using the convention shown in the diagram. Assign port 6 untagged.

6) Create the VLAN **bbone1**, give it an IP address in the 10.0.1.**0**/24 network, using the convention shown in the diagram. Assign ports 1 and 4 untagged (port 1 will be used to connect the workstation).

7) Create the OSPF area **10.17.0.0** and area **10.19.0.0** using the CLI command: **create ospf area.**

8) Display the IP configuration statistics for the VLAN **norm171**.

   What two flags must be set to YES for OSPF to work on this VLAN?

   _____

9) Enable the VLANs **norm171**, **norm191**, and **bbone1** for OSPF by adding it to area **10.17..0,** area **10.19..0,** and area **0.0.0.0** respectively using the CLI command **config ospf add vlan_name area <area_id>**.

   What warning message do you get when you add the VLAN to the OSPF area?

   _____

   What do you need to do before routing will work?

   _____

10) Enable IP forwarding for the VLAN **norm171**, **norm191**, and **bbone1**.

11) What command displays the state of the OSPF routing protocol? _____

12) Enable the OSPF routing protocol for the switch.

13) Save the newly created switch configuration to the secondary file location.

14) Display the OSPF area information.

    How many areas are configured on the switch? _____

    How many interfaces are in the area 10.17.0.0? _____

    What is the state of the interface(s) in area 10.17.0.0 and what does it stand for?

    _____

15) Connect port 6 on switch OSPF_LAB_5 to port 5 on switch OSPF_LAB_6, port 5 on switch OSPF_LAB_5 to port 6 on OSPF_LAB_4, and port 4 on OSPF_LAB_5 to port 4 on OSPF_LAB_2.

_____

Lab15 – OSPF Configuration I

SW5

16) Once all the switches are cabled together, display the OSPF information for the VLAN **norm171** using the CLI command **show ospf interface <vlan_name>.**

What is the router ID for the Designated Router? _____

What is the IP Address for the Designated Router?_____

Is the ID and the IP address for the Designated Router different or the same? Why is it?

_____

_____

What is the state of the neighbor connection? _____

17) Display the area information for 10.17.0.0

What is the state of the interface in the area 10.17.0.0 and what does it mean?

_____

18) Configure the laptop with the following parameters:

IP Address = 10.0.1.202
IP Mask = 255.255.255.0
Gateway = 10.0.1.2

19) Connect the laptop to Port 1 on switch OSPF_LAB_5.

20) Ping the gateway interface from the laptop.

Is the ping successful? _____

21) Ping the interfaces 10.11.1.2 and 10.13.1.2. Is the ping successful?_____

This completes Lab 15 – OSPF Configuration I – Switch 5

Lab15 – OSPF Configuration I

SW6

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Setup and configure a network with the topology provided. Create VLANs as shown.
2. Create an OSPF area and add a VLAN to it using the CLI command: **create ospf area, config ospf add.**
3. Determine what is required for routing to work and what to enable for OSPF to work on a VLAN.
4. Display the area information using the CLI command: **sh ospf area all.**
5. Configure the laptop and add it to the configured network running OSPF and verify via PING if the connection works.

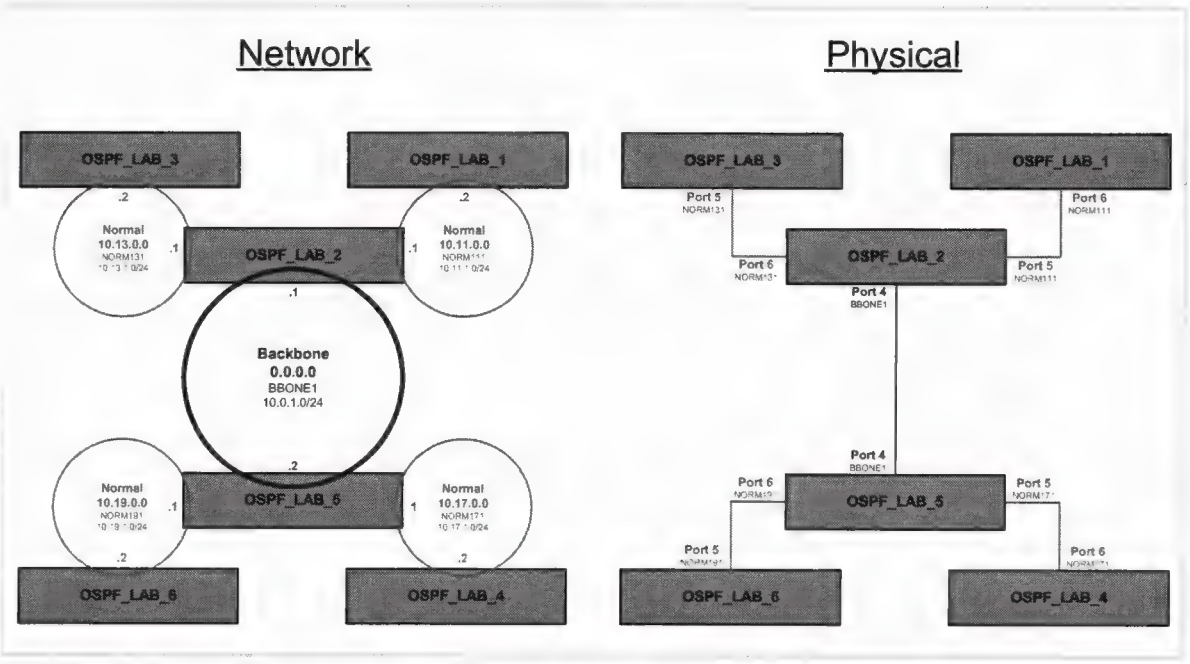
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: *Switch Station 6*



1) Clear the switch of all old configuration information. Then Logon as admin.

2) Name the switch according to the following template: OSPF_LAB_<*switch number*>

3) Delete all ports out of the default VLAN **default**.

Lab15 – OSPF Configuration I

4) Create the VLAN **norm191**, give it an IP address in the 10.19.1.0/24 network, using the convention shown in the diagram. Assign ports 1 and 5 (port 1 will be used to connect the workstation).

5) Create the OSPF area **10.19.0.0** using the CLI command: **create ospf area.**

6) Display the IP configuration statistics for the VLAN **norm191**.

   What two flags must be set to YES for OSPF to work on this VLAN?

   _____

7) Enable the VLAN **norm191** for OSPF by adding it to area **10.19.0.0** using the CLI command **config ospf add vlan_name area <area_id>**.

   What warning message do you get when you add the VLAN to the OSPF area?

   _____

   What do you need to do before routing will work?

   _____

8) Enable IP forwarding for the VLAN **norm191**.

9) What command displays the state of the OSPF routing protocol? _____

   Enable the OSPF routing protocol for the switch.

10) Save the newly created switch configuration to the secondary file location.

11) Display the OSPF area information.

    How many areas are configured on the switch? _____

    How many interfaces are in the area 10.19.0.0? _____

    What is the state of the interface(s) in area 10.19.0.0 and what does it stand for?

    _____

12) Connect port 35 on switch OSPF_LAB_6 to port 26 on switch OSPF_LAB_5.

13) Once all the switches are cabled together, display the OSPF information for the VLAN **norm191** using the CLI command **show ospf interface <vlan_name>.**

    What is the router ID for the Designated Router? _____

    What is the IP Address for the Designated Router?_____

    Is the ID and the IP address for the Designated Router different or the same? Why is it?

    _____

    _____

_____

Lab15 – OSPF Configuration I

SW6

What is the state of the neighbor connection? _____

14) Display the area information for 10.19.0.0

What is the state of the interface in the area 10.19.0.0 and what does it mean?

_____

15) Configure the laptop with the following parameters:

IP Address = 10.19.1.201
IP Mask = 255.255.255.0
Gateway = 10.19.1.2

16) Connect the laptop to Port 1 on switch OSPF_LAB_6.

17) Ping the gateway interface from the laptop.

Is the ping successful? _____

18) Ping the interface 10.17.1.2 from the laptop.

Is the ping successful? _____

19) Change the laptop gateway to 10.19.1.1.

20) Ping the interface 10.17.1.2 from the laptop.

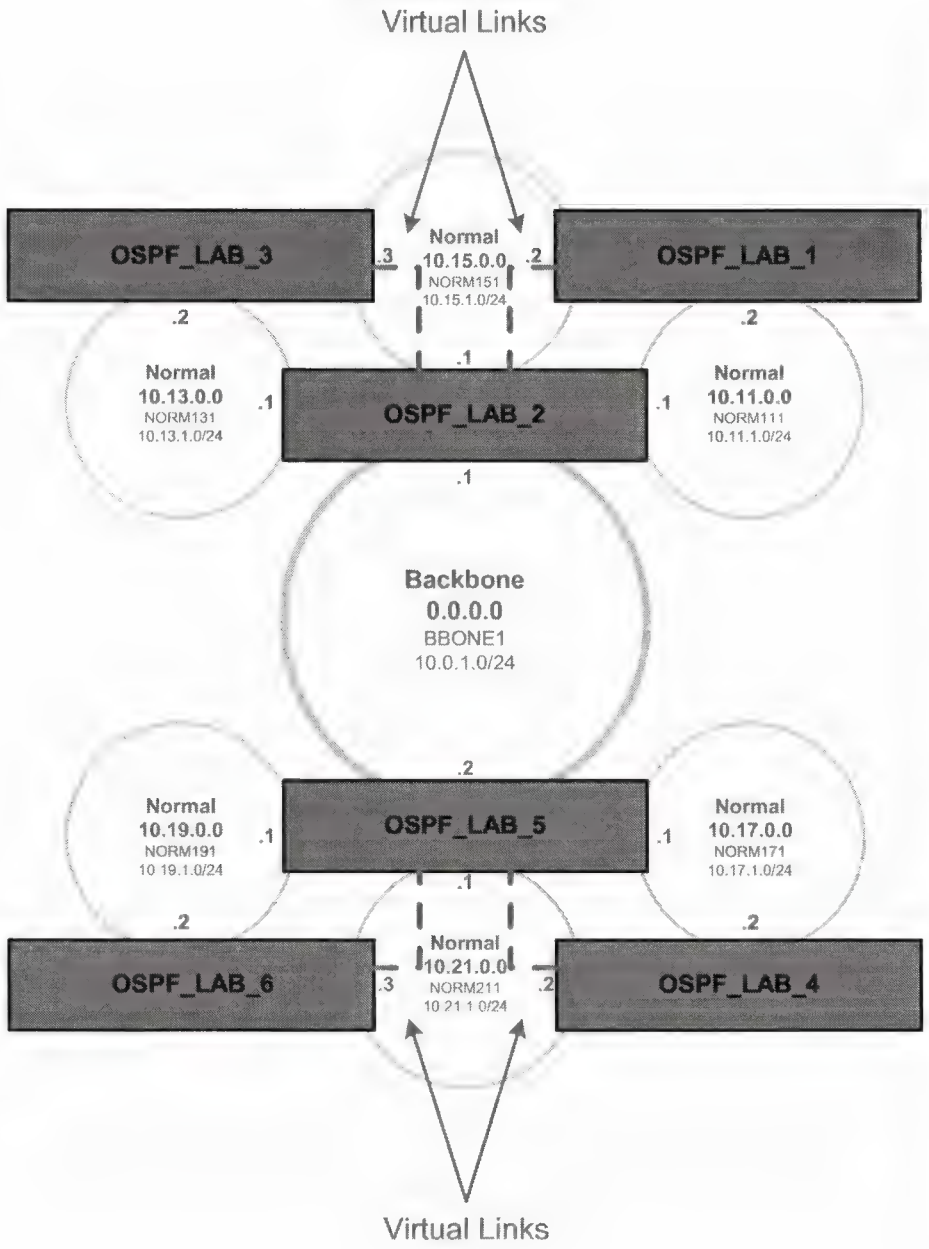
Is the ping successful? _____

This completes Lab 15 – OSPF Configuration I – Switch 6

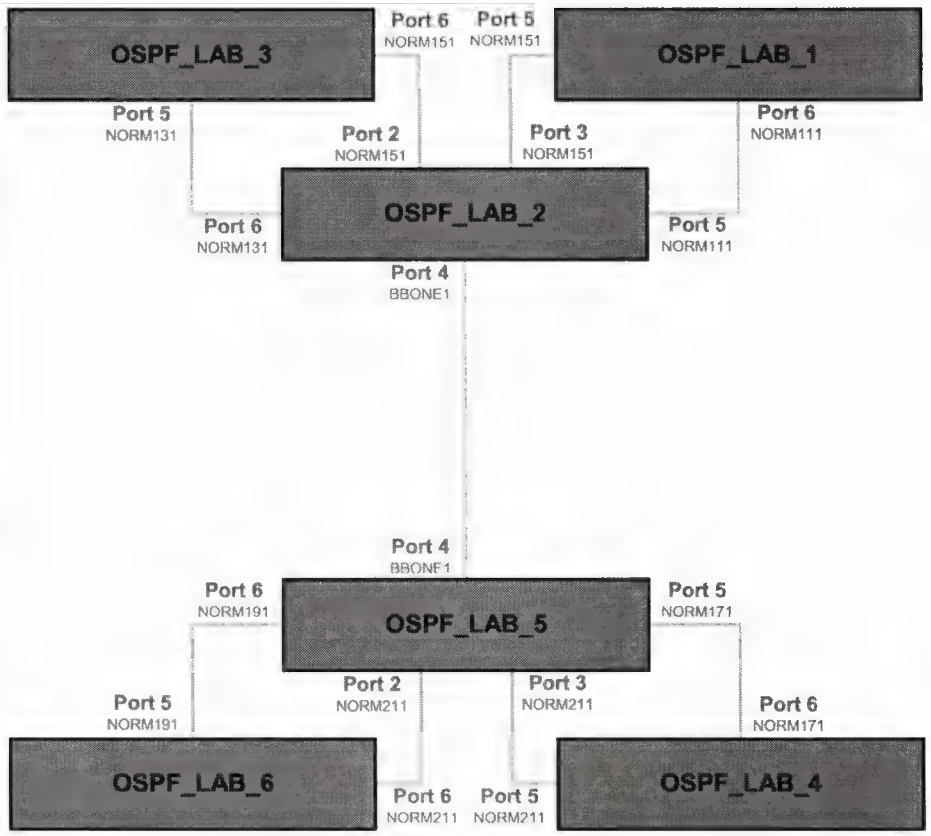
_____

Lab16b – OSPF Configuration II

Network

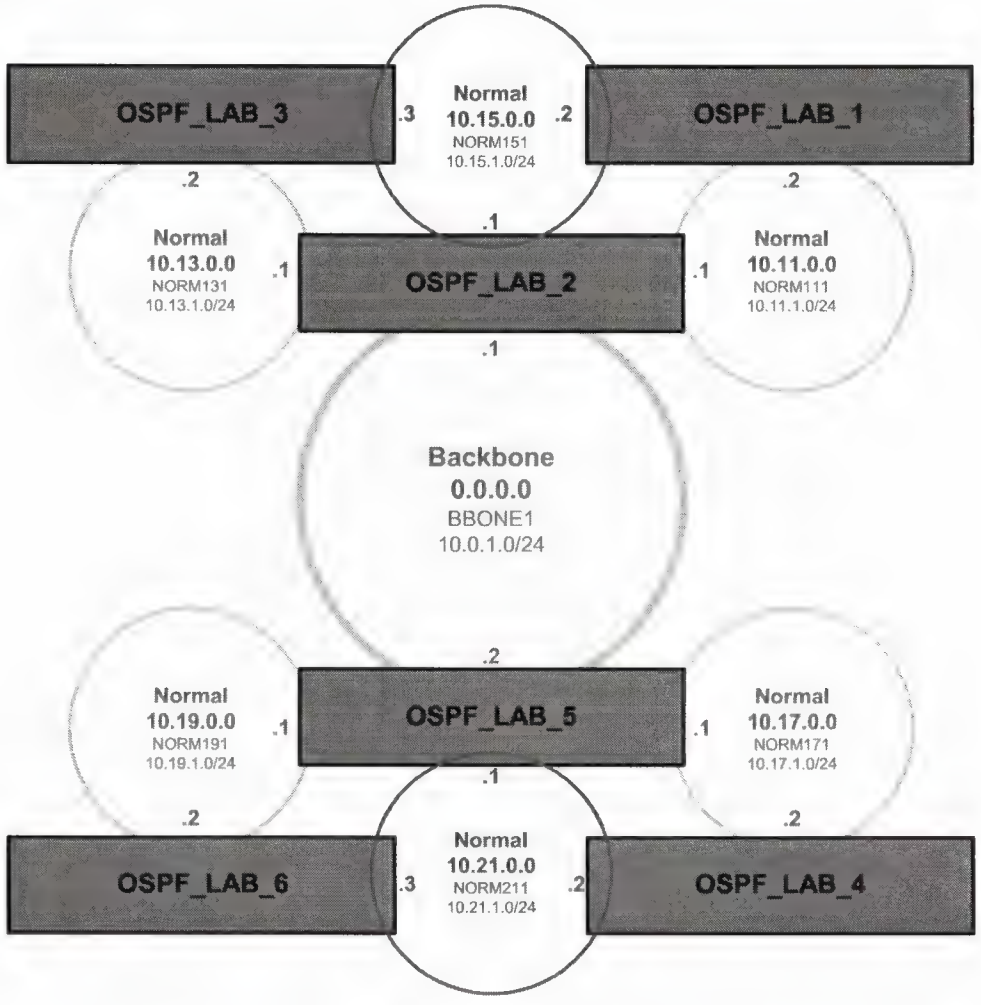


Physical

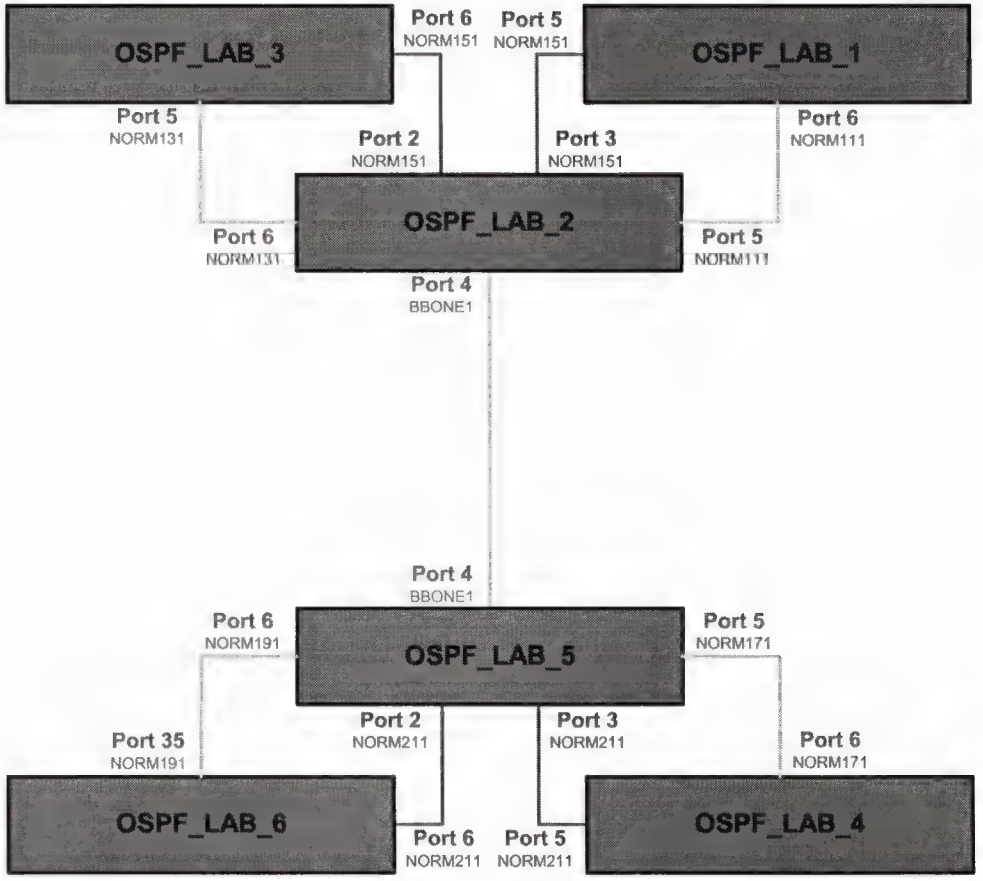


Lab16a – OSPF Configuration II

Network



Physical



Lab16 – OSPF Configuration II

SW1

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Create a new OSPF area and add new vlans continuing with the previous Lab
2. Be familiar with adding and displaying virtual links with the CLI ·**config ospf add virtual-link** and·**show ospf virtual-link** Verify and confirm why a virtual link between ABRs may be necessary.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: ***Switch Station 1***

NOTE: This Lab exercise is a continuation of Lab 17. Utilize the same switch orientation you are working on. Reboot the switch to have the saved configuration from the previous Lab Exercise.

1) Using the CLI, logon to the switch as an ADMIN and verify that the existing setup from Lab 17 is stable. Verify with all your neighbors.

2) Create the VLAN **norm151** and assign it an IP address in the 10.15.1.**N**/24 network.

3) Configure to add port 5 untagged to the VLAN **norm151**.

4) Enable IP Forwarding on VLAN **norm151**.

5) Create a new area with area_id of 10.15.0.0.

6) Enable OSPF for VLAN **norm151** and associate (move) it to the area 10.15.0.0.

7) Display the IP Route Table.

How many learned routes are displayed? _____

8) Display the **IP Route** table again.

How many learned routes are displayed now? _____

What happened to the learned routes?

_____

_____

_____

Lab16 □OSPF Configuration II

SW1

Ensure that all your physical cables are setup and connected properly.

You will now be configuring a Virtual Link between the ABR OSPF_LAB_1 and the backbone area using the CLI command **config ospf add virtual link**

9) Configure a virtual link between OSPF_LAB_1 and OSPF_LAB_2 across area 10.15.0.0.

10) Verify that OSPF_LAB_2 neighbor has already created a virtual link towards you. You can display ospf virtual links with the CLI command : **show ospf virtual link** .

11) Display the **IP Route Table.**

How many learned routes are displayed now? _____

What is the significance of a successful virtual link configuration?

_____

_____

12) Save your new configuration changes to be used for the next Lab.

This completes Lab 16□ OSPF Configuration II□ Switch 1

Lab16 □OSPF Configuration II

SW2

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Create a new OSPF area and add new vlans continuing with the previous Lab
2. Be familiar with adding and displaying virtual links with the CLI ·**config ospf add virtual-link** and·**show ospf virtual-link** Verify and confirm why a virtual link between ABRs may be necessary.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: ***Switch Station 2***

NOTE: This Lab exercise is a continuation of Lab 17. Utilize the same switch orientation you are working on. Reboot the switch to have the saved configuration from the previous Lab Exercise.

1) Using the CLI, logon to the switch as an ADMIN and verify that the existing setup from Lab 17 is stable. Verify with all your neighbors.

2) Create the VLAN **norm151** and assign it an IP address in the 10.15.1.**N**/24 network.

3) Configure to add ports 2 and 3 untagged to the VLAN **norm151**.

4) Enable IP Forwarding on VLAN **norm151**.

5) Create a new area with area_id of 10.15.0.0.

6) Enable OSPF for VLAN **norm151** and have it to belong to area 10.15.0.0.

7) Display the IP Route Table.

How many learned routes are displayed? _____

8) Ensure that all your physical cables are setup and connected properly.

You will now be configuring two Virtual Links between the ABR OSPF_LAB_1 and ABR OSPF_LAB_3 using the CLI command **config ospf add virtual link**

9) Configure a virtual link between OSPF_LAB_2 and OSPF_LAB_1 across area 10.15.0.0. Configure a virtual link between OSPF_LAB_2 and OSPF_LAB_3 across area 10.15.0.0.

10) Verify that OSPF_LAB_1 and OSPF_LAB_3 neighbors have already created a virtual link towards you. You can display ospf virtual links with the CLI command : **show ospf virtual link** .

Lab16 – OSPF Configuration II

SW

11) Display the **IP Route Table.**

How many learned routes are displayed now? _____

What is the significance of a successful virtual link configuration?

_____

_____

12) Save your new configuration changes to be used for the next Lab.

This completes Lab 16 – OSPF Configuration II – Switch 2

Lab16 □OSPF Configuration II

SW3

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Create a new OSPF area and add new vlans continuing with the previous Lab
2. Be familiar with adding and displaying virtual links with the CLI ·**config ospf add virtual-link** and·**show ospf virtual-link** Verify and confirm why a virtual link between ABRs may be necessary.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: ***Switch Station 3***

NOTE: This Lab exercise is a continuation of Lab 17. Utilize the same switch orientation you are working on. Reboot the switch to have the saved configuration from the previous Lab Exercise.

1) Using the CLI, logon to the switch as an ADMIN and verify that the existing setup from Lab 17 is stable. Verify with all your neighbors.

2) Create the VLAN **norm151** and assign it an IP address in the 10.15.1.**N**/24 network.

3) Configure to add port 6 untagged to the VLAN **norm151**.

4) Enable IP Forwarding on VLAN **norm151**.

5) Create a new area with area_id of 10.15.0.0.

6) Enable OSPF for the VLAN **norm151** and have it belong to the area 10.15.0.0.

7) Display the IP Route Table.

   How many learned routes are displayed? _____

8) Display the **IP Route** table again.

   How many learned routes are displayed now? _____

   What happened to the learned routes?

   _____

   _____

   _____

Lab16 – OSPF Configuration II

Ensure that all your physical cables are setup and connected properly.

You will now be configuring a Virtual Link between the ABR OSPF_LAB_3 and the backbone area using the CLI command **config ospf add virtual link**

9) Configure a virtual link between OSPF_LAB_3 and OSPF_LAB_2 across area 10.15.0.0.

10) Verify that OSPF_LAB_2 neighbor has already created a virtual link towards you. You can display ospf virtual links with the CLI command : **show ospf virtual link** .

11) Display the **IP Route Table.**

How many learned routes are displayed now? _____

What is the significance of a successful virtual link configuration?

_____

_____

12) Save your new configuration changes to be used for the next Lab.

This completes Lab 16– OSPF Configuration II– Switch 3

Lab16 – OSPF Configuration II

SW4

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Create a new OSPF area and add new vlans continuing with the previous Lab
2. Be familiar with adding and displaying virtual links with the CLI ·**config ospf add virtual-link** and·**show ospf virtual-link** Verify and confirm why a virtual link between ABRs may be necessary.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: ***Switch Station 4***

NOTE: This Lab exercise is a continuation of Lab 17. Utilize the same switch orientation you are working on. Reboot the switch to have the saved configuration from the previous Lab Exercise.

1) Using the CLI, logon to the switch as an ADMIN and verify that the existing setup from Lab 17 is stable. Verify with all your neighbors.

2) Create the VLAN **norm211** and assign it an IP address in the 10.21.1.**N** /24 network.

3) Configure to add port 5 untagged to the VLAN **norm211**.

4) Enable IP Forwarding on VLAN **norm211**.

5) Create a new area with area_id of 10.21.0.0

6) Enable OSPF for VLAN **norm211** and associate (move) it to the area 10.21.0.0.

7) Display the IP Route Table.

How many learned routes are displayed? none

8) Display the **IP Route** table again.

How many learned routes are displayed now? none

What happened to the learned routes?

There is no virtual link

Lab16 – OSPF Configuration II

Ensure that all your physical cables are setup and connected properly.

You will now be configuring a Virtual Link between the ABR OSPF_LAB_4 and the backbone area using the CLI command **config ospf add virtual link +** IP of router + (10.21.0.0)

9) Configure a virtual link between OSPF_LAB_4 and OSPF_LAB_5 across area 10.21.0.0

10) Verify that OSPF_LAB_5 neighbor has already created a virtual link towards you. You can display ospf virtual links with the CLI command : **show ospf virtual link** .

11) Display the **IP Route Table.**

How many learned routes are displayed now? _____

What is the significance of a successful virtual link configuration?

_____

_____

12) Save your new configuration changes to be used for the next Lab.

This completes Lab 16– OSPF Configuration II– Switch 4

Lab16 – OSPF Configuration II

SW5

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Create a new OSPF area and add new vlans continuing with the previous Lab
2. Be familiar with adding and displaying virtual links with the CLI ·**config ospf add virtual-link** and·**show ospf virtual-link** Verify and confirm why a virtual link between ABRs may be necessary.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: ***Switch Station 5***

NOTE: This Lab exercise is a continuation of Lab 17. Utilize the same switch orientation you are working on. Reboot the switch to have the saved configuration from the previous Lab Exercise.

1) Using the CLI, logon to the switch as an ADMIN and verify that the existing setup from Lab 17 is stable. Verify with all your neighbors.

2) Create the VLAN **norm211** and assign it an IP address in the 10.21.1.**N**/24 network.

3) Configure to add ports 2 and 3 untagged to the VLAN **norm211**.

4) Enable IP Forwarding on VLAN **norm211**.

5) Create a new area with area_id of 10.21.0.0.

6) Enable OSPF for VLAN **norm211** and have it to belong to area 10.21.0.0.

7) Display the IP Route Table.

How many learned routes are displayed? _____

8) Ensure that all your physical cables are setup and connected properly.

You will now be configuring two Virtual Links between the ABR OSPF_LAB_4 and ABR OSPF_LAB_6 using the CLI command **config ospf add virtual link**

9) Configure a virtual link between OSPF_LAB_5 and OSPF_LAB_4 across area 10.21.0.0. Configure a virtual link between OSPF_LAB_5 and OSPF_LAB_6 across area 10.21.0.0.

10) Verify that OSPF_LAB_4 and OSPF_LAB_6 neighbors have already created a virtual link towards you. You can display ospf virtual links with the CLI command : **show ospf virtual link** .

Lab16 – OSPF Configuration II

11) Display the **IP Route Table.**

How many learned routes are displayed now? _____

What is the significance of a successful virtual link configuration?

_____

_____

12) Save your new configuration changes to be used for the next Lab.

This completes Lab 16 – OSPF Configuration II – Switch 5

Lab16 – OSPF Configuration

SW6

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Create a new OSPF area and add new vlans continuing with the previous Lab
2. Be familiar with adding and displaying virtual links with the CLI ·**config ospf add virtual-link** and·**show ospf virtual-link** Verify and confirm why a virtual link between ABRs may be necessary.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: ***Switch Station 6***

NOTE: This Lab exercise is a continuation of Lab 17. Utilize the same switch orientation you are working on. Reboot the switch to have the saved configuration from the previous Lab Exercise.

1) Using the CLI, logon to the switch as an ADMIN and verify that the existing setup from Lab 17 is stable. Verify with all your neighbors.

2) Create the VLAN **norm211** and assign it an IP address in the 10.21.1.**N** /24 network.

3) Configure to add port 6 untagged to the VLAN **norm211**.

4) Enable IP Forwarding on VLAN **norm211**.

5) Create a new area with area_id of 10.21.0.0

6) Enable OSPF for VLAN **norm211** and associate (move) it to the area 10.21.0.0.

7) Display the IP Route Table.

How many learned routes are displayed? _____

8) Display the **IP Route** table again.

How many learned routes are displayed now? _____

What happened to the learned routes?

_____

_____

_____

_____

Lab16 – OSPF Configuration

Ensure that all your physical cables are setup and connected properly.

You will now be configuring a Virtual Link between the ABR OSPF_LAB_6 and the backbone area using the CLI command **config ospf add virtual link**

9) Configure a virtual link between OSPF_LAB_6 and OSPF_LAB_5 across area 10.21.0.0

10) Verify that OSPF_LAB_5 neighbor has already created a virtual link towards you. You can display ospf virtual links with the CLI command : **show ospf virtual link** .

11) Display the **IP Route Table.**

How many learned routes are displayed now? _____

What is the significance of a successful virtual link configuration?

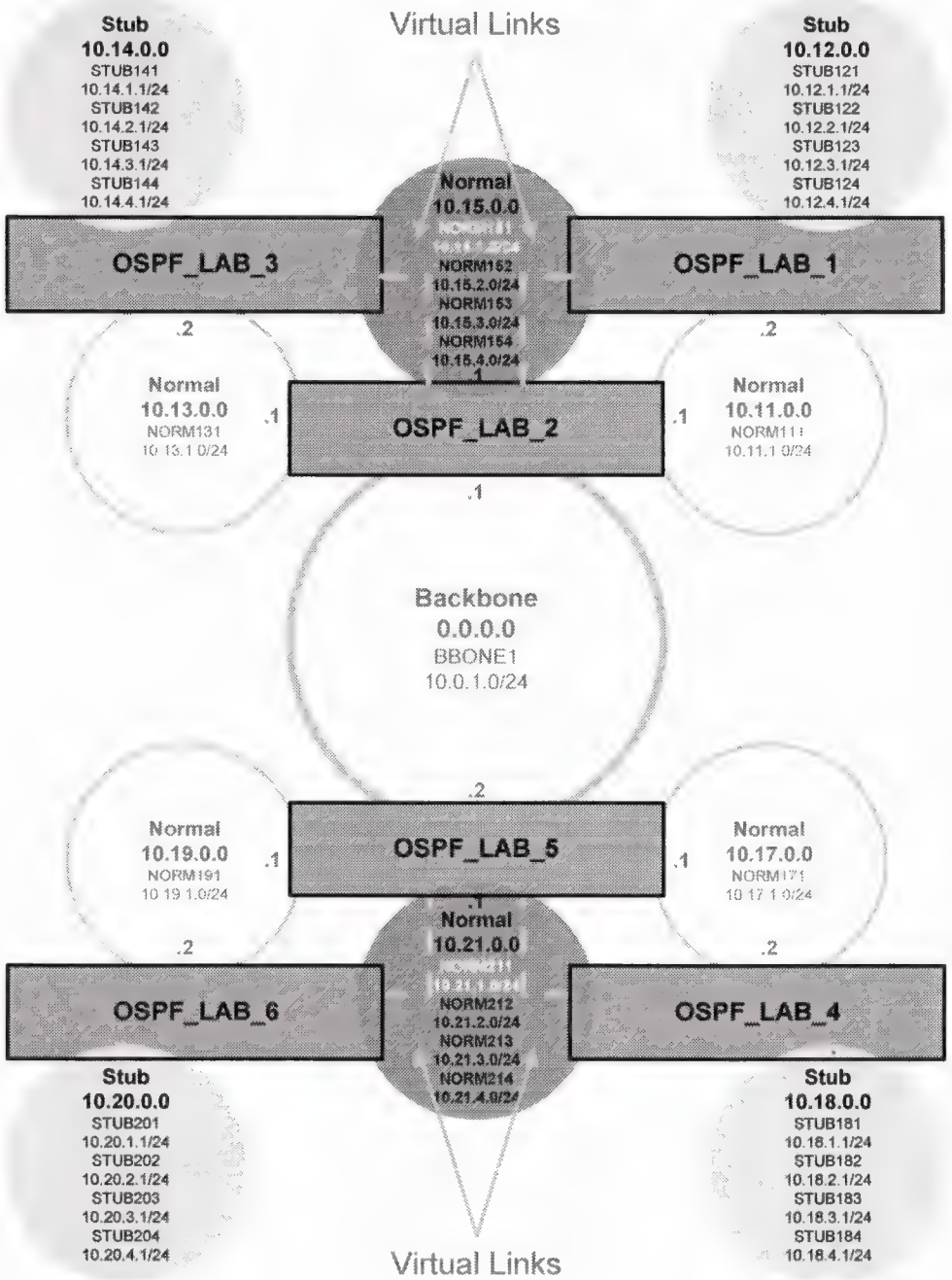
_____

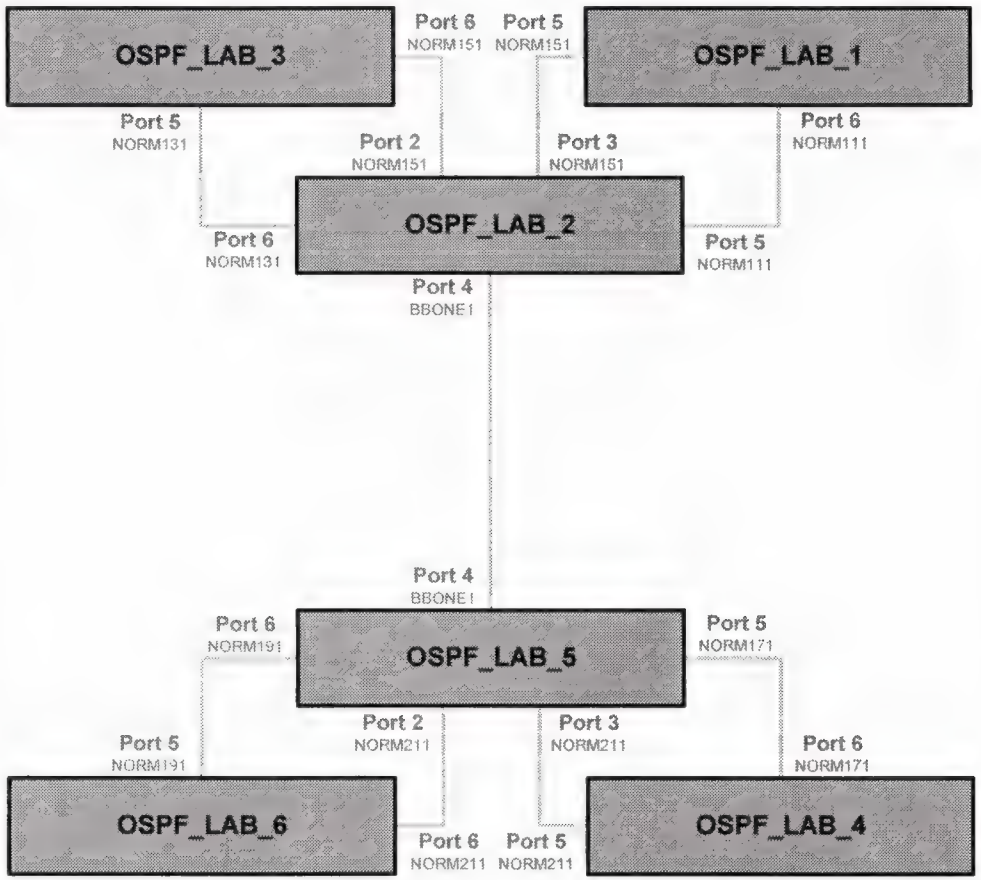
_____

12) Save your new configuration changes to be used for the next Lab.

This completes Lab 16– OSPF Configuration II– Switch 6

Lab17 – OSPF Configuration III





Lab17 – OSPF Configuration III

SW1

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Be familiar with the CLI commands for creating and configuring different types of areas – normal, stub, nssa and using the previous setup.
2. Using the CLI, expound on the configuration of the OSPF network by creating more OSPF area and adding more VLANs to it.
3. Create 34-39 routes utilizing 4 cross-connect cables for setting up dummy interfaces.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: ***Switch Station 1***

NOTE: This Lab exercise is a continuation of Lab 18. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) Create the following VLANs:

   stub121 with IP address 10.12.1.1/24 with a tag of 10
   stub122 with IP address 10.12.2.1/24 with a tag of 20
   stub123 with IP address 10.12.3.1/24 with a tag of 30
   stub124 with IP address 10.12.4.1/24 with a tag of 40

2) Create the OSPF area 10.12.0.0 and add the VLANs **stub121**, **stub122**, **stub123**, and **stub124** to it.

3) Configure the new area 10.12.0.0 as a summarized stub area with a default cost of 5.

4) Display the area information for 10.12.0.0. What is the area type? _____

5) Enable the VLANs **stub121**, **stub122**, **stub123**, and **stub124** with the OSPF routing protocol.

6) Enable IP forwarding for the VLANs **stub121**, **stub122**, **stub123**, and **stub124**.

7) Is it possible to ping any of the newly created interfaces **stub121**, **stub122**, **stub123**, or **stub124**?

_____

Lab17 – OSPF Configuration III

8) Display the IP configuration information for VLAN **stub121**. What is the interface status?

_____

9) Add port 1, tagged, to each of the vlans **stub121**, **stub122**, **stub123**, **stub124**.

10) Display the IP configuration information for VLAN **stub121** again. What is the status of the interface?

_____

11) Is it now possible to ping the IP addresses of the interfaces **stub121**, **stub122**, **stub123**, or **stub124**?

_____

12) Save the modified switch configuration to the secondary file location.

This completes Lab 17 – OSPF Configuration - III– Switch 1

Lab17 – OSPF Configuration III

SW2

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Be familiar with the CLI commands for creating and configuring different types of areas – normal, stub, nssa and using the previous setup.
2. Using the CLI, expound on the configuration of the OSPF network by creating more OSPF area and adding more VLANs to it.
3. Create 34-39 routes utilizing 4 cross-connect cables for setting up dummy interfaces.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: ***Switch Station 2***

NOTE: This Lab exercise is a continuation of Lab 18. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) Create the following VLANs:

norm152 with IP address 10.15.2.1/24 with a tag of 20
norm153 with IP address 10.15.3.1/24 with a tag of 30
norm154 with IP address 10.15.4.1/24 with a tag of 40

2) Add the VLANs **norm152**, **norm153**, and **norm154** to the OSPF area 10.15.0.0.

3) Enable the VLANs **norm152**, **norm153**, and **norm154** with the OSPF routing protocol.

4) Enable IP forwarding for the VLANs **norm152**, **norm153**, and **norm154**.

5) Is it possible to ping any of the newly created VLANs **norm152**, **norm153**, or **norm154**?

_____

6) Display the IP configuration information for VLAN **norm152**.

What is the interface status?

_____

_____

Lab17 – OSPF Configuration III

7) Add port 1, tagged, to each of the new VLANs **norm152**, **norm153**, and **norm154**.

8) Display the IP configuration information for VLAN **norm152** again. What is the status of the interface?

9) Is it now possible to ping the IP addresses of the interfaces **norm152**, **norm153**, or **norm154**?

10) Save the modified switch configuration to the secondary file location.

This completes Lab17 – OSPF Configuration - III – Switch 2

Lab17 – OSPF Configuration III

SW3

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Be familiar with the CLI commands for creating and configuring different types of areas – normal, stub, nssa and using the previous setup.
2. Using the CLI, expound on the configuration of the OSPF network by creating more OSPF area and adding more VLANs to it.
3. Create 34-39 routes utilizing 4 cross-connect cables for setting up dummy interfaces.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: *Switch Station 3*

NOTE: This Lab exercise is a continuation of Lab 18. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) Create the following VLANs:

stub141 with IP address 10.14.1.1/24 with a tag of 10
stub142 with IP address 10.14.2.1/24 with a tag of 20
stub143 with IP address 10.14.3.1/24 with a tag of 30
stub144 with IP address 10.14.4.1/24 with a tag of 40

2) Create the OSPF area 10.14.0.0 and add the VLANs **stub141**, **stub142**, **stub143**, and **stub144** to it.

3) Configure the new area 10.14.0.0 as a summarized stub area with a default cost of 5.

4) Display the area information for 10.14.0.0. What is the area type? _____

5) Enable the VLANs **stub141**, **stub142**, **stub143**, and **stub144** with the OSPF routing protocol.

6) Enable IP forwarding for the VLANs **stub141**, **stub142**, **stub143**, and **stub144**.

Lab17 – OSPF Configuration III

7) Is it possible to ping any of the newly created interfaces **stub141**, **stub142**, **stub143**, or **stub144**?

---

8) Display the IP configuration information for VLAN **stub141**. What is the interface status?

---

9) Add port 1, tagged, to the new VLANs **stub141**, **stub142**, **stub143**, and **stub144**.

10) Display the IP configuration information for VLAN **stub141** again. What is the status of the interface?

---

11) Is it now possible to ping the IP addresses of the interfaces **stub141**, **stub142**, **stub143**, or **stub144**?

---

12) Save the modified switch configuration to the secondary file location.

This completes Lab 17 – OSPF Configuration - III– Switch 3

Lab17 – OSPF Configuration III

SW4

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Be familiar with the CLI commands for creating and configuring different types of areas – normal, stub, nssa and using the previous setup.
2. Using the CLI, expound on the configuration of the OSPF network by creating more OSPF area and adding more VLANs to it.
3. Create 34-39 routes utilizing 4 cross-connect cables for setting up dummy interfaces.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: ***Switch Station 4***

NOTE: This Lab exercise is a continuation of Lab 18. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) Create the following VLANs:

stub181 with IP address 10.18.1.1/24 with a tag of 10
stub182 with IP address 10.18.2.1/24 with a tag of 20
stub183 with IP address 10.18.3.1/24 with a tag of 30
stub184 with IP address 10.18.4.1/24 with a tag of 40

2) Create the OSPF area 10.18.0.0 and add the VLANs **stub181**, **stub182**, **stub183**, and **stub184** to it.

3) Configure the new area 10.18.0.0 as a summarized stub area with a default cost of 5.

4) Display the area information for 10.18.0.0. What is the area type? STub Summ ~~Normal~~

5) Enable the VLANs **stub181**, **stub182**, **stub183**, and **stub184** with the OSPF routing protocol.

6) Enable IP forwarding for the VLANs **stub181**, **stub182**, **stub183**, and **stub184**.

Lab17 – OSPF Configuration III

SW

7) Is it possible to ping any of the newly created interfaces **stub181**, **stub182**, **stub183**, or **stub184**?

no

8) Display the IP configuration information for VLAN **stub181**. What is the interface status?

down

9) Add port 1, tagged, to each of the new VLANs **stub181**, **stub182**, **stub183**, and **stub184**.

10) Display the IP configuration information for VLAN **stub181** again. What is the status of the interface?

up

11) Is it now possible to ping the IP addresses of the interfaces **stub181**, **stub182**, **stub183**, or **stub184**?

yes

12) Save the modified switch configuration to the secondary file location.

This completes Lab 17 – OSPF Configuration - III– Switch 4

Lab17 – OSPF Configuration III

SW5

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Be familiar with the CLI commands for creating and configuring different types of areas – normal, stub, nssa and using the previous setup.
2. Using the CLI, expound on the configuration of the OSPF network by creating more OSPF area and adding more VLANs to it.
3. Create 34-39 routes utilizing 4 cross-connect cables for setting up dummy interfaces.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: ***Switch Station 5***

NOTE: This Lab exercise is a continuation of Lab 18. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) Create the following VLANs:

norm 212 with IP address 10.21.2.1/24 with a tag of 20
norm 213 with IP address 10.21.3.1/24 with a tag of 30
norm 214 with IP address 10.21.4.1/24 with a tag of 40

2) Add the VLANs **norm 212**, **norm 213**, and **norm 214** to the OSPF area 10.21.0.0.

3) Enable the VLANs **norm 212**, **norm 213**, and **norm 214** with the OSPF routing protocol.

4) Enable IP forwarding for the VLANs **norm 212**, **norm 213**, and **norm 214**.

5) Is it possible to ping any of the newly created VLANs **norm 212**, **norm 213**, or **norm 214**?

_____

6) Display the IP configuration information for VLAN **norm 212**.

What is the interface status?

_____

_____

Lab17 – OSPF Configuration III

7) Add port 1 tagged to each of the new VLANs **norm 212**, **norm 213**, or **norm 214**.

8) Display the IP configuration information for VLAN **norm 212** again. What is the status of the interface?

9) Is it now possible to ping the IP addresses of the interfaces **norm 212**, **norm 213**, or **norm 214**?

10) Save the modified switch configuration to the secondary file location.

This completes Lab 17 – OSPF Configuration - III – Switch 5

Lab17 – OSPF Configuration III

SW6

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Be familiar with the CLI commands for creating and configuring different types of areas – normal, stub, nssa and using the previous setup.
2. Using the CLI, expound on the configuration of the OSPF network by creating more OSPF area and adding more VLANs to it.
3. Create 34-39 routes utilizing 4 cross-connect cables for setting up dummy interfaces.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES: ***Switch Station 6***

NOTE: This Lab exercise is a continuation of Lab 18. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) Create the following VLANs:

stub201 with IP address 10.20.1.1/24 with a tag of 10
stub202 with IP address 10.20.2.1/24 with a tag of 20
stub203 with IP address 10.20.3.1/24 with a tag of 30
stub204 with IP address 10.20.4.1/24 with a tag of 40

2) Create the OSPF area 10.20.0.0 and add the VLANs **stub201**, **stub202**, **stub203**, and **stub204** to it.

3) Configure the new area 10.20.0.0 as a summarized stub area with a default cost of 5.

4) Display the area information for 10.20.0.0. What is the area type? _____

5) Enable the VLANs **stub201**, **stub202**, **stub203**, and **stub204** with the OSPF routing protocol.

6) Enable IP forwarding for the VLANs **stub201**, **stub202**, **stub203**, and **stub204**.

Lab17 – OSPF Configuration III

7) Is it possible to ping any of the newly created interfaces **stub201**, **stub202**, **stub203**, or **stub204**?

---

8) Display the IP configuration information for VLAN **stub201**. What is the interface status?

---

9) Add port 1, tagged, to each of the new VLANs **stub201**, **stub202**, **stub203**, or **stub204**.

10) Display the IP configuration information for VLAN **stub201** again. What is the status of the interface?

---

11) Is it now possible to ping the IP addresses of the interfaces **stub201**, **stub202**, **stub203**, or **stub204**?

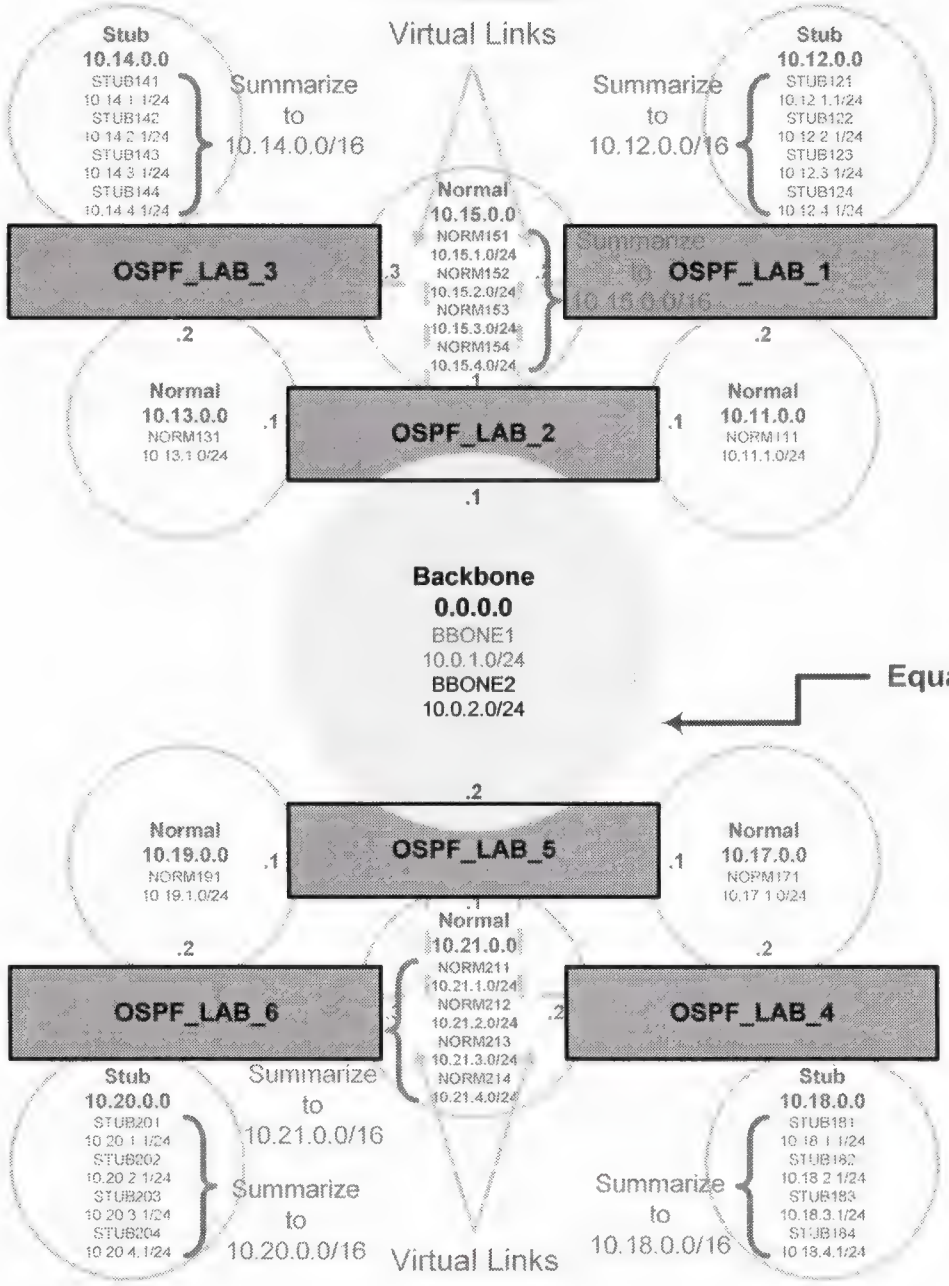
---

12) Save the modified switch configuration to the secondary file location.

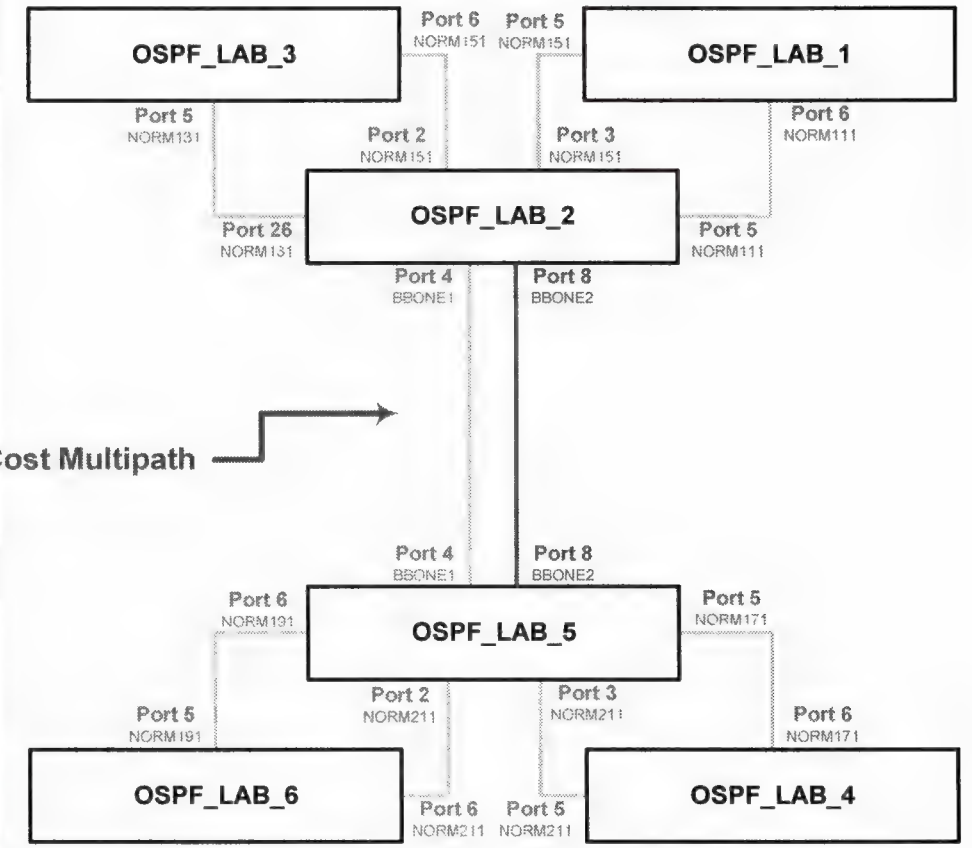
This completes Lab 17 – OSPF Configuration - III– Switch 6

Lab18 – OSPF Configuration IV

Network



Physical



config OSPF area area-id add range
ipaddress MASK type-3
- config

Lab18 – OSPF Configuration IV

SW1

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Using the CLI, expound on the configuration of the OSPF network utilizing the CLI command: **config ospf routeid, config ospf add virtual link, config ospf area add range,** and display ospf virtual-link.
2. While enabling/disabling OSPF, change parameters and then verify the total number of routes that were added using CLI command: **show iproute**.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Student Guide
2. Summit Switch User Guide (if available)

PROCEDURES: *Switch Station 1*

NOTE: This Lab exercise is a continuation of Lab 19. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) From the command line, display the IP routing table.

How many routes are displayed? _____

2) Flush the OSPF environment by disabling (turning off) and enabling (turning on) the OSPF protocol.

3) Display the IP route table again. Has it changed? _____

Why? _____

_____

Why did the router ID change?

_____

_____

4) Disable OSPF. Change the router ID to the value 10.10.10.10 and then enable OSPF again.

5) Change the virtual link to reflect the new router ID of the neighbor router.

_____

Lab18 – OSPF Configuration IV

6) Display the virtual link information and look at the VL state. If the STATE condition is not FULL, you may need to cycle OSPF in series with the neighbor router.

7) Display the IP routing table. Have all the routes been restored? _____

8) Save the modified switch configuration to the secondary file location.

9) Display the IP route table and record the total number of routes displayed: _____

10) Summarize the routes in area 10.12.0.0 to the address range 10.12.0.0/16 and advertise it as a type-3 (OSPF-internal) LSA.

11) When all of the routers have had their assigned areas summarized, display the IP routing table.
Has the routing table been altered? _____

12) From the IP route table, list out all of the summarized routes:

_____

13) Save the modified switch configuration to the secondary file location.

This completes Lab18 – OSPF Configuration - IV– Switch 1

Lab18 – OSPF Configuration IV

SW2

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Using the CLI, expound on the configuration of the OSPF network utilizing the CLI command: **config ospf routeid, config ospf add virtual link, config ospf area add range,** and display ospf virtual-link.
2. While enabling/disabling OSPF, change parameters and then verify the total number of routes that were added using CLI command: **show iproute**.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Student Guide
2. Summit Switch User Guide (if available)

PROCEDURES: *Switch Station 2*

NOTE: This Lab exercise is a continuation of Lab 19. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) From the command line, display the IP routing table.

How many routes are displayed? _____

2) Flush the OSPF environment by disabling (turning off) and enabling (turning on) the OSPF protocol.

3) Display the IP route table again. Has it changed? _____

Why? _____

_____

Why did the router ID change?

_____

_____

4) Disable OSPF. Change the router ID to the value 20.20.20.20 and enable OSPF again.

5) Change the virtual links to reflect the new router ID of the neighbor router.

_____

Lab18 – OSPF Configuration IV

6) Display the virtual link information and look at the VL state. If the STATE condition is not FULL, you may need to cycle OSPF in series with the neighbor router.

7) Display the IP routing table. Have all the routes been restored? _____

8) Save the modified switch configuration to the secondary file location.

9) Display the IP route table and record the total number of routes displayed: _____

10) Summarize the routes in area 10.15.0.0 to the address range 10.15.0.0/16 and advertise it as a type-3 (OSPF-internal) LSA.

11) When all of the routers have had their assigned areas summarized, display the IP routing table.
Has the routing table been altered? _____

12) From the IP route table, list out all of the summarized routes:

_____

Add an equal-cost multipath connection between OSPF_LAB_2 and OSPF_LAB_5 across the backbone.

13) Create a new VLAN named **bbone2**, add port 8, and assign it an IP address in the 10.0.2.0/24 subnet.

14) Add **bbone2** to the backbone area and enable IP forwarding and OSPF routing on the VLAN.

15) Enable IP route sharing on the switch.

16) Save the modified switch configuration to the secondary file location.

This completes Lab 18 – OSPF Configuration - IV– Switch 2

Lab18 – OSPF Configuration IV

SW3

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Using the CLI, expound on the configuration of the OSPF network utilizing the CLI command: **config ospf routeid, config ospf add virtual link, config ospf area add range,** and display ospf virtual-link.
2. While enabling/disabling OSPF, change parameters and then verify the total number of routes that were added using CLI command: **show iproute**.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Student Guide
2. Summit Switch User Guide (if available)

PROCEDURES: *Switch Station 3*

NOTE: This Lab exercise is a continuation of Lab 19. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) From the command line, display the IP routing table.

How many routes are displayed? _____

2) Flush the OSPF environment by disabling (turning off) and enabling (turning on) the OSPF protocol.

3) Display the IP route table again. Has it changed? _____

Why? _____

_____

Why did the router ID change?

_____

_____

4) Disable OSPF. Change the router ID to the value 30.30.30.30 and enable OSPF again.

5) Change the virtual link to reflect the new router ID of the neighbor router.

_____

Lab18 – OSPF Configuration IV

6) Display the virtual link information and look at the VL state. If the STATE condition is not FULL, you may need to cycle OSPF in series with the neighbor router.

7) Display the IP routing table. Have all the routes been restored? _____

8) Save the modified switch configuration to the secondary file location.

9) Display the IP route table and record the total number of routes displayed: _____

10) Summarize the routes in area 10.14.0.0 to the address range 10.14.0.0/16 and advertise it as a type-3 (OSPF-internal) LSA.

11) When all of the routers have had their assigned areas summarized, display the IP routing table.
Has the routing table been altered? _____

12) From the IP route table, list out all of the summarized routes:

_____

13) Save the modified switch configuration to the secondary file location.

This completes Lab18 – OSPF Configuration - IV– Switch 3

Lab18 – OSPF Configuration IV

SW4

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Using the CLI, expound on the configuration of the OSPF network utilizing the CLI command: **config ospf routeid, config ospf add virtual link, config ospf area add range,** and display ospf virtual-link.
2. While enabling/disabling OSPF, change parameters and then verify the total number of routes that were added using CLI command: **show iproute**.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Student Guide
2. Summit Switch User Guide (if available)

PROCEDURES: *Switch Station 4*

NOTE: This Lab exercise is a continuation of Lab 19. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) From the command line, display the IP routing table.

How many routes are displayed? 10 (7 direct route + 3 OSPF intra

2) Flush the OSPF environment by disabling (turning off) and enabling (turning on) the OSPF protocol.

3) Display the IP route table again. Has it changed? 7 direct routes

Why? The entry has been flushed out.

Why did the router ID change?

4) Disable OSPF. Change the router ID to the value 40.40.40.40 and enable OSPF again.

5) Change the virtual link to reflect the new router ID of the neighbor router.

Lab18 – OSPF Configuration IV

6) Display the virtual link information and look at the VL state. If the STATE condition is not FULL, you may need to cycle OSPF in series with the neighbor router.

7) Display the IP routing table. Have all the routes been restored? : _____

8) Save the modified switch configuration to the secondary file location.

9) Display the IP route table and record the total number of routes displayed: 23

10) Summarize the routes in area 10.18.0.0 to the address range 10.18.0.0/16 and advertise it as a type-3 (OSPF-internal) LSA.

11) When all of the routers have had their assigned areas summarized, display the IP routing table.
Has the routing table been altered? _____

12) From the IP route table, list out all of the summarized routes:

10

13) Save the modified switch configuration to the secondary file location.

This completes Lab18 – OSPF Configuration - IV– Switch 4

Lab18 – OSPF Configuration IV

SW5

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Using the CLI, expound on the configuration of the OSPF network utilizing the CLI command: **config ospf routeid, config ospf add virtual link, config ospf area add range,** and display ospf virtual-link.
2. While enabling/disabling OSPF, change parameters and then verify the total number of routes that were added using CLI command: **show iproute**.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Student Guide
2. Summit Switch User Guide (if available)

PROCEDURES: *Switch Station 5*

NOTE: This Lab exercise is a continuation of Lab 19. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) From the command line, display the IP routing table.

How many routes are displayed? _____

2) Flush the OSPF environment by disabling (turning off) and enabling (turning on) the OSPF protocol.

3) Display the IP route table again. Has it changed? _____

Why? _____

_____

Why did the router ID change?

_____

_____

4) Disable OSPF. Change the router ID to the value 50.50.50.50 and enable OSPF again.

5) Change the virtual links to reflect the new router ID of the neighbor router.

_____

Lab18 – OSPF Configuration IV

6) Display the virtual link information and look at the VL state. If the STATE condition is not FULL, you may need to cycle OSPF in series with the neighbor router.

7) Display the IP routing table. Have all the routes been restored? _____

8) Save the modified switch configuration to the secondary file location.

9) Display the IP route table and record the total number of routes displayed: _____

10) Summarize the routes in area 10.21.0.0 to the address range 10.21.0.0/16 and advertise it as a type-3 (OSPF-internal) LSA.

11) When all of the routers have had their assigned areas summarized, display the IP routing table.
Has the routing table been altered? _____

12) From the IP route table, list out all of the summarized routes:

_____

Add an equal-cost multipath connection between OSPF_LAB_5 and OSPF_LAB_2 across the backbone.

13) Create a new VLAN named **bbone2**, add port 8, and assign it an IP address in the 10.0.2.0/24 subnet.

14) Add **bbone2** to the backbone area and enable IP forwarding and OSPF routing on the VLAN.

15) Enable IP route sharing on the switch.

16) Save the modified switch configuration to the secondary file location.

This completes Lab 18 – OSPF Configuration - IV– Switch 5

Lab18 – OSPF Configuration IV

SW6

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Using the CLI, expound on the configuration of the OSPF network utilizing the CLI command: **config ospf routeid, config ospf add virtual link, config ospf area add range,** and display ospf virtual-link.
2. While enabling/disabling OSPF, change parameters and then verify the total number of routes that were added using CLI command: **show iproute**.

MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required

REFERENCES:

1. Lab procedures from the Student Guide
2. Summit Switch User Guide (if available)

PROCEDURES: *Switch Station 6*

NOTE: This Lab exercise is a continuation of Lab 19. Utilize the same switch orientation you are working on and follow the network topology provided. Be sure to boot the switch using the configuration of the previous lab before proceeding.

1) From the command line, display the IP routing table.

How many routes are displayed? _____

2) Flush the OSPF environment by disabling (turning off) and enabling (turning on) the OSPF protocol.

3) Display the IP route table again. Has it changed? _____

Why? _____

_____

Why did the router ID change?

_____

_____

4) Disable OSPF. Change the router ID to the value 60.60.60.60 and enable OSPF again.

5) Change the virtual link to reflect the new router ID of the neighbor router.

_____

Lab18 – OSPF Configuration IV

6) Display the virtual link information and look at the VL state. If the STATE condition is not FULL, you may need to cycle OSPF in series with the neighbor router.

7) Display the IP routing table. Have all the routes been restored? _____

8) Save the modified switch configuration to the secondary file location.

9) Display the IP route table and record the total number of routes displayed: _____

10) Summarize the routes in area 10.20.0.0 to the address range 10.20.0.0/16 and advertise it as a type-3 (OSPF-internal) LSA.

11) When all of the routers have had their assigned areas summarized, display the IP routing table.
Has the routing table been altered? _____

12) From the IP route table, list out all of the summarized routes:

_____

13) Save the modified switch configuration to the secondary file location.

This completes Lab18 – OSPF Configuration - IV– Switch 6

Lab19 – ESRP Configuration

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Setup a network for ESRP configuration.
2. Understand the use of the following CLI commands: **show edp, show iparp, clear iparp, show fdb, clear fdb, show esrp, enable esrp vlan, configure vlan esrp priority** .

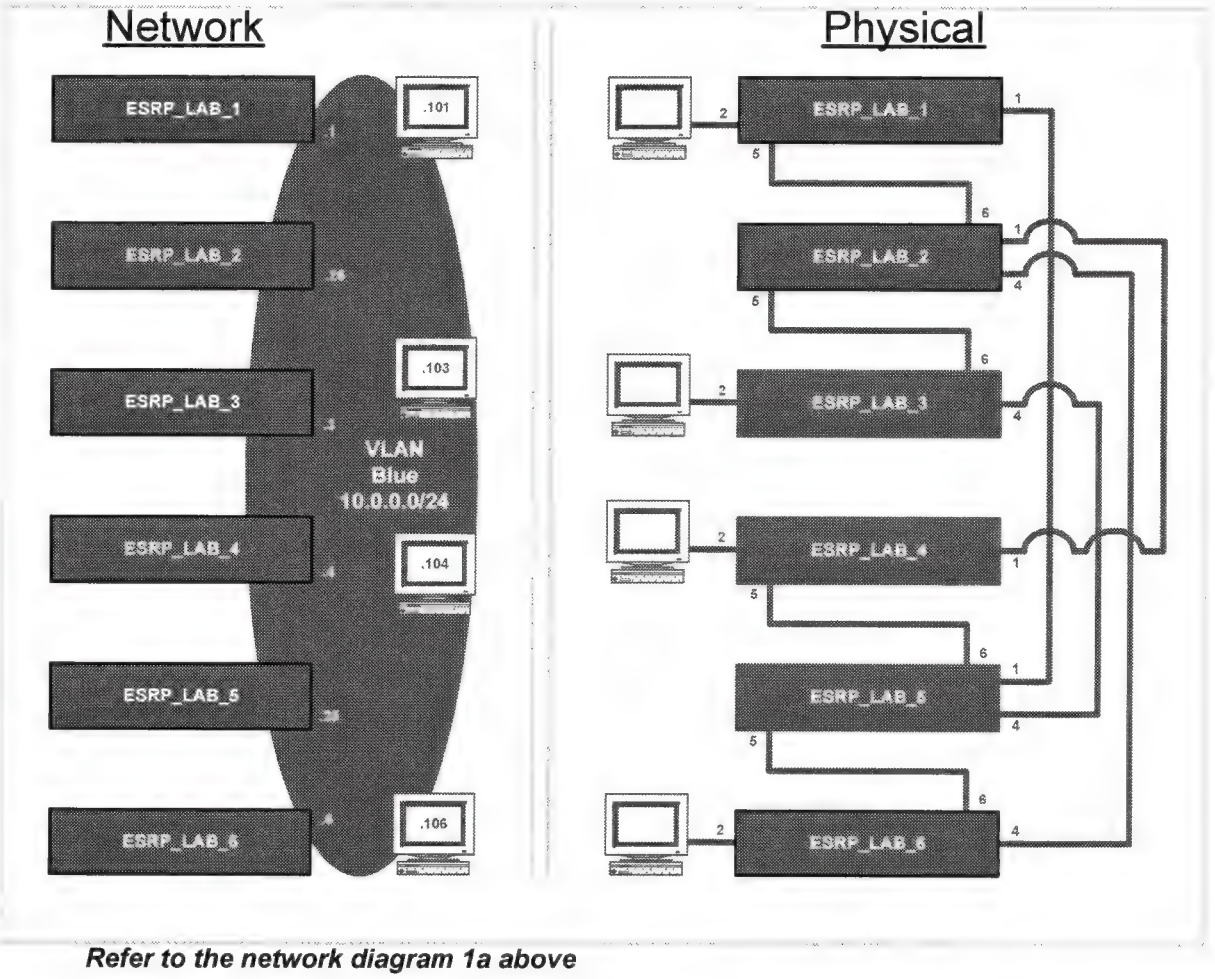
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable.

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:



Refer to the network diagram 1a above

Lab19 – ESRP Configuration

1) Clear the switch of all old configuration information. Remove all cables connected from previous labs.

2) Name the switch according to the following template: ESRP_LAB_<*switch number*>

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue,** give it an IP address in the 10.0.0.0/24 network, and assign ports 1, 2 and 5.

5) Using CAT5 cross-over patch cables, connect the following:
port 5 on ESRP_LAB_1 to port 6 on ESRP_LAB_2
port 1 on ESRP_LAB_1 to port 1 on ESRP_LAB_5
the laptop to port 2 on ESRP_LAB_1

Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (7)

6) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 and note which of the two switches is the ESRP master switch for the VLAN blue , and which is the slave switch.

Master: 5

Slave: 2

7) Display the EDP information for switch ESRP_LAB_1 using the CLI command.

Q: How many systems are displayed?

---

8) From your switch console, ping the **blue** interface of ESRP_LAB_3, ESRP_LAB_4, and ESRP_LAB_6.

Q: Which, if any, pings are successful?

---

9) Display the ARP table on switch ESRP_LAB_1 from the switch console and note the MAC address for each of the interface addresses pinged in (8).

10) Display the forwarding database on ESRP_LAB_1.

Q: Which port is associated with the MAC addresses recorded in (9)?

Wait for the team configuring the switch configured as Master (determined in step (6)) to turn off their switch before continuing.

11) Flush the ARP table and forwarding database on switch ESRP_LAB_1.

Lab19 – ESRP Configuration

SW1

12) Once again, ping the **blue** interface of ESRP_LAB_3, ESRP_LAB_4, and ESRP_LAB_6 from the switch console.

Q: Which pings are successful, if any?

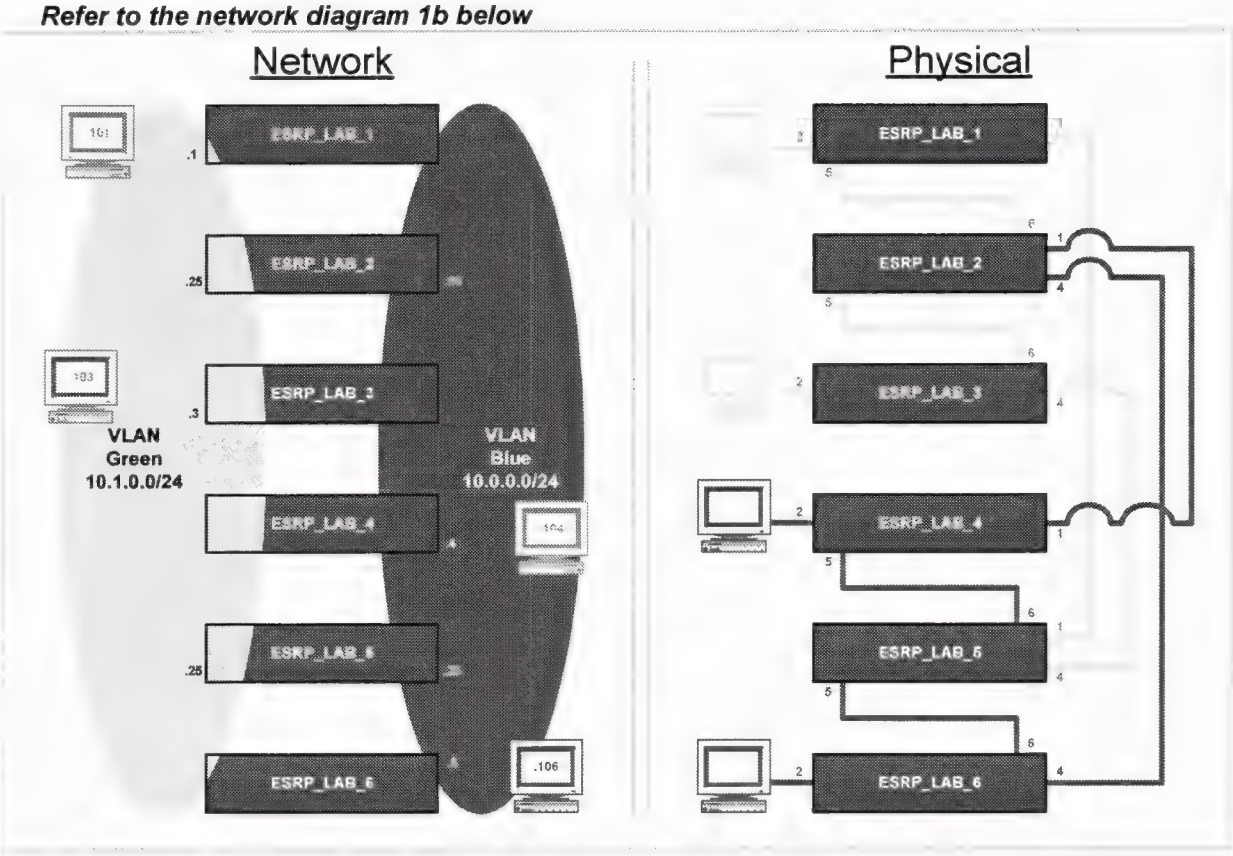
---

13) Now display the forwarding database on ESRP_LAB_1.

Q: Which port is associated with the MAC addresses recorded in (9)?

Wait for the team configuring the switch previously elected as Master to boot their switch before continuing.

Refer to the network diagram 1b below



14) Delete the **blue** VLAN from switch ESRP_LAB_1

15) Create the VLAN **green,** give it an IP address in the 10.1.0.0/24 network, and assign ports 1 and 5.

Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (15)

16) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 and note which of the two switches is the ESRP master switch for both of the VLANs **blue** and **green**.

Lab19 – ESRP Configuration

Master: _____

Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (17)

17) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 once more and note which of the two switches is the ESRP master switch for the VLAN **blue** , which is the ESRP master switch for the VLAN **green**, and which switches are flagged as slave.

BLUE Master: _____ **BLUE** Slave: _____

GREEN Master: _____ **GREEN** Slave: _____

18) From the console, ping the **green** interface on ESRP_LAB_3.

19) Display the forwarding database on ESRP_LAB_1.

Q: Which port is associated with the MAC address of ESRP_LAB_3?

_____

20) Disconnect the appropriate cable connected to the **green** master switch noted in (25) above.

21) Once more, ping the **green** interface on ESRP_LAB_3 from the console.

22) Display the forwarding database on ESRP_LAB_1.

Q: Which port is associated with the MAC address of ESRP_LAB_3?

_____

This completes Lab19 – ESRP Configuration Lab – Switch 1

Lab19 – ESRP Configuration

SW2

1) Clear the switch of all old configuration information. Remove all cables connected from previous labs.

2) Name the switch according to the following template: ESRP_LAB_<*switch number*>

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue,** give it an IP address in the 10.0.0.0/24 network, and assign ports 1, 4, 5 and 6.

5) Using CAT5 cross-over patch cables, connect the following:
port 5 on ESRP_LAB_2 to port 6 on ESRP_LAB_3
port 6 on ESRP_LAB_2 to port 5 on ESRP_LAB_1
port 1 on ESRP_LAB_2 to port 1 on ESRP_LAB_4
port 4 on ERP_LAB_2 to port 4 on ESRP_LAB_6.

6) Enable the Extreme Standby Router Protocol on the **blue** VLAN.

7) Display the esrp information on switch ESRP_LAB_2 using the CLI command – **show esrp**.

   Which is the master esrp switch for VLAN **blue**?

   Note the switch name of the Master and Slave switch below:

   Master: _____

   Slave: _____

8) Display the EDP information for switch ESRP_LAB_2 using the CLI command - **show edp**.

   Q: How many systems are displayed?

   _____

9) From your switch console, ping the **blue** interface of ESRP_LAB_1, ESRP_LAB_3, ESRP_LAB_4 and ESRP_LAB_6.

   Q: Which, if any, pings are successful?

   _____

10) If ESRP_LAB_2 is the Master switch noted in (7) above, turn the switch off and proceed to the end of step (12).

11) If ESRP_LAB_2 was the Slave switch noted in (7) above, wait about 10 seconds and then display the esrp information on switch ESRP_LAB_2.

   *Q: Which is the master esrp switch for VLAN **blue**?*

   _____

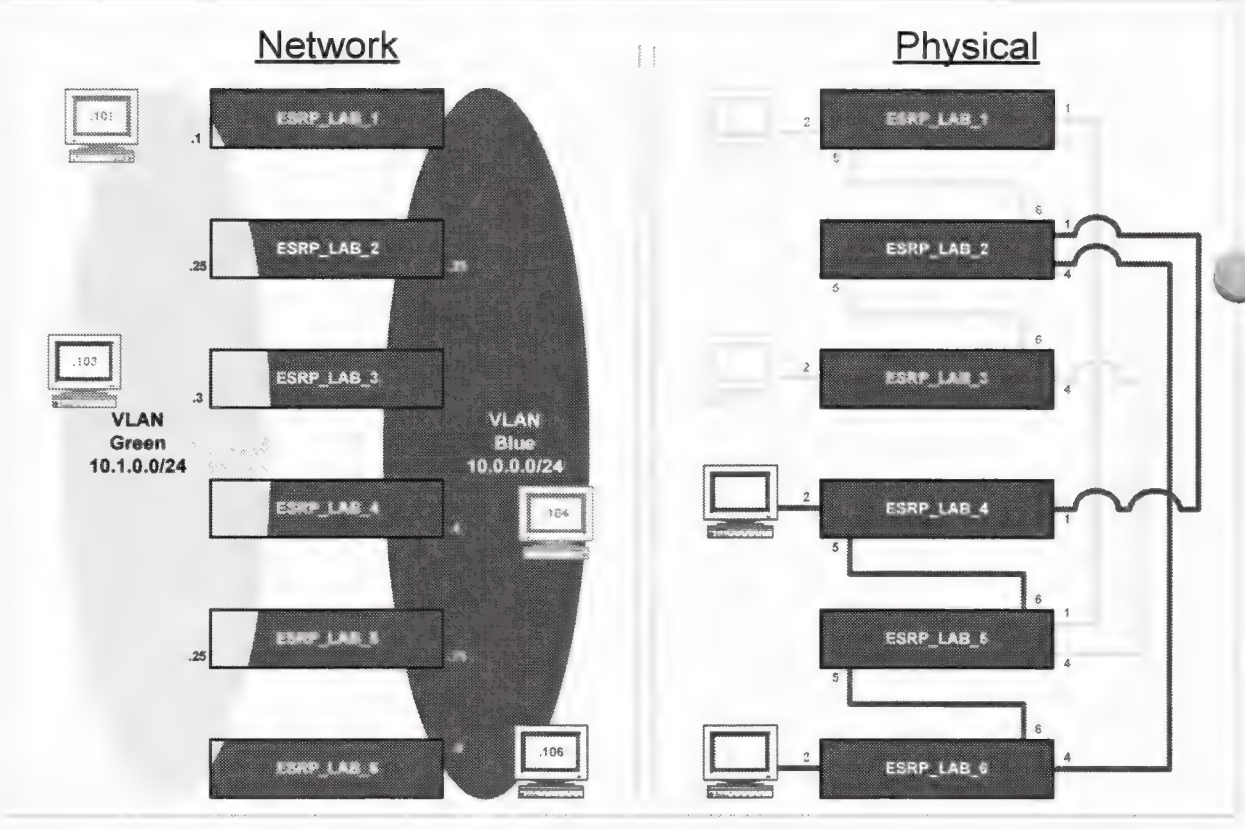
12) From your switch console, ping the **blue** interface of ESRP_LAB_1, ESRP_LAB_3, ESRP_LAB_4, and ESRP_LAB_6 again.

_____

Q: Which, if any, pings are successful?

Wait for the team configuring the switch previously elected as Master to boot their switch before continuing.

Refer to the network diagram 1b below



13) Delete ports 5 and 6 from VLAN **blue**.

14) Create the VLAN **green,** give it an IP address in the 10.1.0.0/24 network, and assign ports 5 and 6.

15) Enable ESRP for the new VLAN **green** using the CLI command – **enable esrp vlan <vlan_name>**

Before proceeding, confirm that the teams on ESRP_LAB_1 and ESRP_LAB_3 have completed step (15)

16) Display the esrp information on switch ESRP_LAB_2.

*Q: Which is the master esrp switch for VLAN **blue** and **green**?*

Note the switch name of the Master switch below:

Lab19 – ESRP Configuration

SW2

Master: _____

Before proceeding, confirm that the teams on ESRP_LAB_1 and ESRP_LAB_3 have completed step (16) and ESRP_LAB_4 and ESRP_LAB_6 have completed step (14)

17) If ESRP_LAB_2 was the Slave switch noted in (11) above, change the esrp priority for VLAN **green** to 10 using the CLI command - **configure vlan <vlan_name> esrp priority <priority> .**

18) Display the esrp information for switch ESRP_LAB_2 and note which of the two switches is the ESRP master switch for the VLAN **blue**, which is the ESRP master switch for the VLAN **green**, and which switches are flagged as slave.

BLUE Master: _____ **BLUE** Slave: _____

GREEN Master: _____ **GREEN** Slave: _____

19) From the console, ping the **green** interface on ESRP_LAB_1 and ESRP_LAB_3.

Q: Which, if any, pings are successful?

_____

20) From the console, ping the **blue** interface on ESRP_LAB_4 and ESRP_LAB_6.

Q: Which, if any, pings are successful?

_____

This completes Lab19 – ESRP Configuration Lab – Switch 2

_____

Lab19 – ESRP Configuration

SW3

1) Clear the switch of all old configuration information. Remove all cables connected from previous labs.

2) Name the switch according to the following template: ESRP_LAB_<*switch number*>

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue,** give it an IP address in the 10.0.0.0/24 network, and assign ports 2, 4, and 6.

5) Using CAT5 cross-over patch cables, connect the following:
port 6 on ESRP_LAB_3 to port 5 on ESRP_LAB_2
connect port 4 on ESRP_LAB_3 to port 4 on ESRP_LAB_5
the laptop to port 2 on ESRP_LAB_3

Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (7)

6) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 and note which of the two switches is the ESRP master switch for the VLAN **blue**, and which is the slave switch.

Master: _____

Slave: _____

7) Display the EDP information for switch ESRP_LAB_3.

Q: How many systems are displayed?

_____

8) From your switch console, ping the **blue** interface of ESRP_LAB_1, ESRP_LAB_4, ESRP_LAB_6.

Q: Which, if any, pings are successful?

_____

9) Display the ARP table on switch ESRP_LAB_3 from the switch console and note the MAC address for each of the interface addresses pinged in (8).

10) Display the forwarding database on ESRP_LAB_3.

Q: Which port is associated with the MAC addresses recorded in (9)?

_____

Wait for the team configuring the switch configured as Master (determined in step (6)) to turn off their switch before continuing.

11) Flush the ARP table and forwarding database on switch ESRP_LAB_3.

12) Once again, ping the **blue** interface of ESRP_LAB_1, ESRP_LAB_4, ESRP_LAB_6 from the switch console.

_____

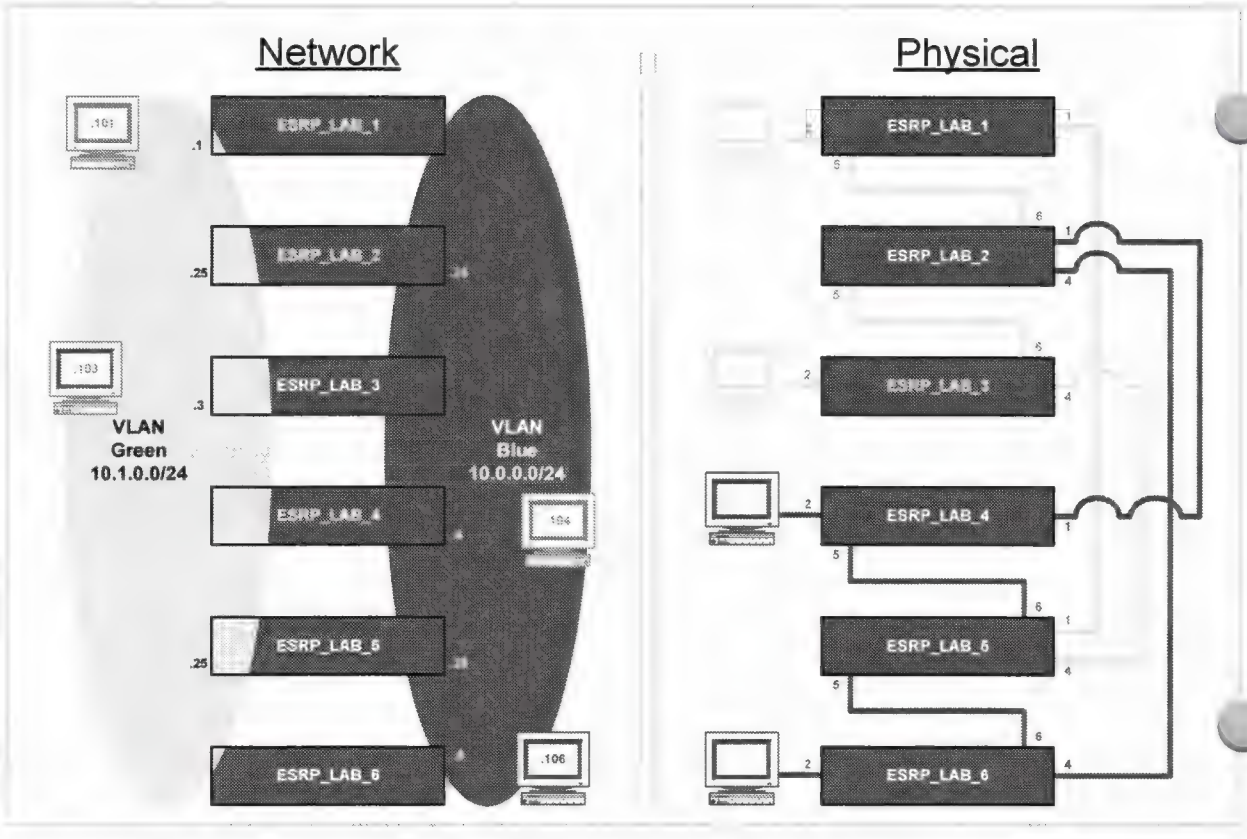
Q: Which, if any, pings are successful?

13) Now display the forwarding database on ESRP_LAB_3.

Q: Which port is associated with the MAC addresses recorded in (9)?

Wait for the team configuring the switch previously elected as Master to boot their switch before continuing.

Refer to the network diagram 1b below



14) Delete the **blue** VLAN from switch ESRP_LAB_3

15) Create the VLAN **green,** give it an IP address in the 10.1.0.0/24 network, and assign ports 2, 4, and 6.

Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (15)

16) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 and note which of the two switches is the ESRP master switch for both of the VLANs **blue** and **green**.

Master: _____

Lab19 – ESRP Configuration

SW3

Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (17)

17) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 once more and note which of the two switches is the ESRP master switch for the VLAN **blue**, which is the ESRP master switch for the VLAN **green**, and which switches are flagged as slave.

BLUE Master: _____ **BLUE** Slave: _____

GREEN Master: _____ **GREEN** Slave: _____

18) From the console, ping the **green** interface on ESRP_LAB_1.

19) Display the forwarding database on ESRP_LAB_3.

Q: Which port is associated with the MAC address of ESRP_LAB_1?

_____

20) Disconnect the appropriate cable connected to the **green** master switch noted in (36) above.

21) Once more, ping the **green** interface on ESRP_LAB_1 from the console,.

22) Display the forwarding database on ESRP_LAB_3.

Q: Which port is associated with the MAC address of ESRP_LAB_1?

_____

This completes Lab19 – ESRP Configuration Lab – Switch 3

Lab19 – ESRP Configuration

SW4

1) Clear the switch of all old configuration information. Remove all cables connected from previous labs.

2) Name the switch according to the following template: ESRP_LAB_<*switch number*>

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue,** give it an IP address in the 10.0.0.0/24 network, and assign ports 1, 2, and 5.

5) Using CAT5 cross-over patch cables, connect the following:
port 5 on ESRP_LAB_4 to port 6 on ESRP_LAB_5
port 1 on ESRP_LAB_4 to port 1 on ESRP_LAB_2
the laptop to port 2 on ESRP_LAB_4

Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (7)

6) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 and note which of the two switches is the ESRP master switch for the VLAN **blue**, and which is the slave switch.

Master: _____

Slave: _____

7) Display the EDP information for switch ESRP_LAB_4.

Q: How many systems are displayed?

1 switch -5

8) From your switch console, ping the **blue** interface of ESRP_LAB_1, ESRP_LAB_3, and ESRP_LAB_6.

Q: Which, if any, pings are successful?

9) Display the ARP table on switch ESRP_LAB_4 from the switch console and note the MAC address for each of the interface addresses pinged in (8).

10) Display the forwarding database on ESRP_LAB_4.

Q: Which port is associated with the MAC addresses recorded in (9)?

(1, 5)

Wait for the team configuring the switch configured as Master (determined in step (6)) to turn off their switch before continuing.

11) Flush the ARP table and forwarding database on switch ESRP_LAB_4.

12) Once again, ping the **blue** interface of ESRP_LAB_1, ESRP_LAB_3, and ESRP_LAB_6 from the switch console.

Can't ping.

Q: Which, if any, pings are successful?

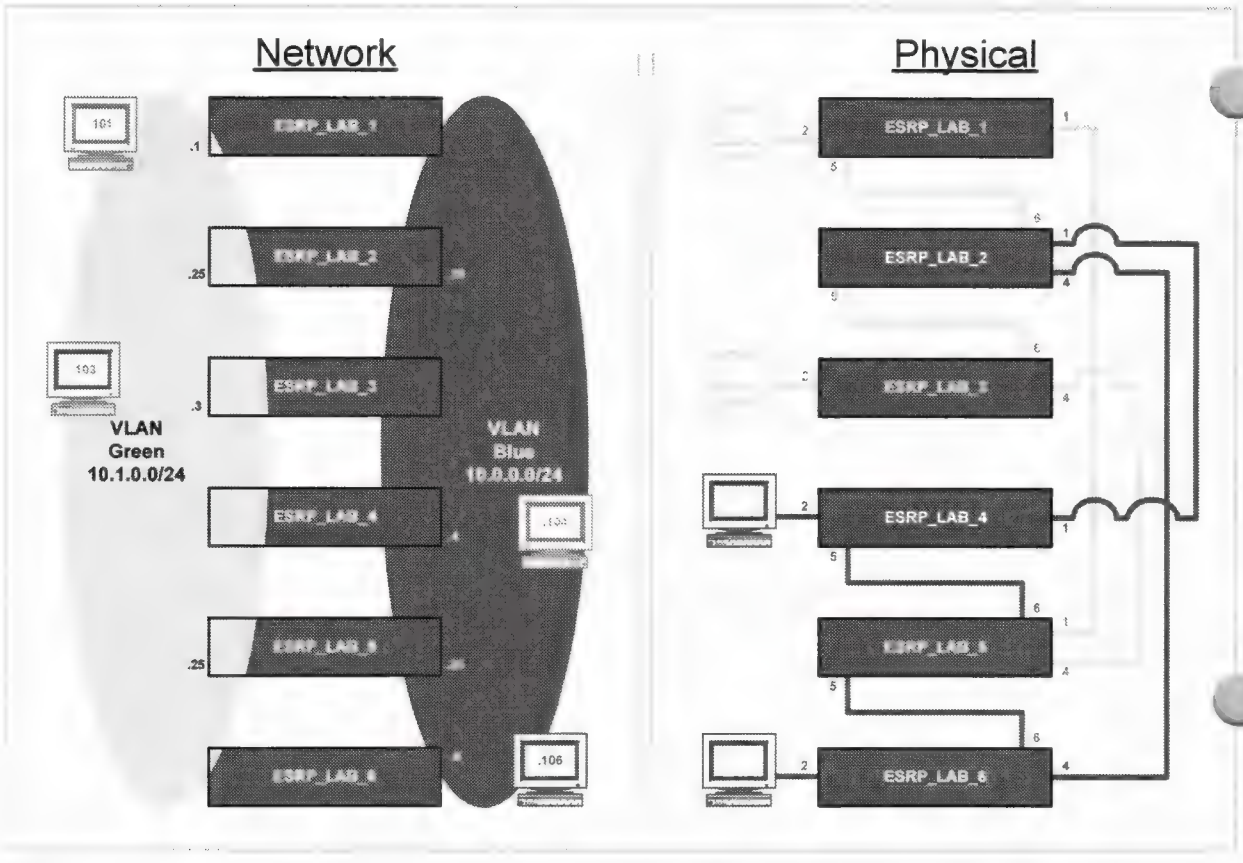
13) Now display the forwarding database on ESRP_LAB_4.

Q: Which port is associated with the MAC addresses recorded in (9)?

port 5

Wait for the team configuring the switch previously elected as Master to boot their switch before continuing.

Refer to the network diagram 1b below



Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (16)

14) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 and note which of the two switches is the ESRP master switch for both of the VLANs **blue** and **green**.

Master: _____

Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (17)

Lab19 – ESRP Configuration

SW4

15) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 once more and note which of the two switches is the ESRP master switch for the VLAN **blue**, which is the ESRP master switch for the VLAN **green**, and which switches are flagged as slave.

BLUE Master: 5 **BLUE** Slave: 2

GREEN Master: 5 **GREEN** Slave: 2

16) From the console, ping the **blue** interface on ESRP_LAB_6. yes

17) Display the forwarding database on ESRP_LAB_4.

Q: Which port is associated with the MAC address of ESRP_LAB_6? port 5

18) Disconnect the appropriate cable connected to the **blue** master switch noted in (25) above. –

19) Once more, ping the **blue** interface on ESRP_LAB_6 from the console,. yes .

20) Display the forwarding database on ESRP_LAB_4.

Q: Which port is associated with the MAC address of ESRP_LAB_6?

1

This completes Lab19 – ESRP Configuration Lab – Switch 4

Lab19 – ESRP Configuration

SW5

1) Clear the switch of all old configuration information. Remove all cables connected from previous labs.

2) Name the switch according to the following template: ESRP_LAB_*<switch number>*

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue,** give it an IP address in the 10.0.0.0/24 network, and assign ports 1, 4, 5 and 6.

5) Using CAT5 cross-over patch cables, connect the following:
port 5 on ESRP_LAB_5 to port 6 on ESRP_LAB_6
port 6 on ESRP_LAB_5 to port 5 on ESRP_LAB_4
port 1 on ESRP_LAB_5 to port 1 on ESRP_LAB_1
port 4 on ESRP_LAB_5 to port 4 on ESRP_LAB_3

6) Enable the Extreme Standby Router Protocol on the **blue** VLAN.

7) Display the esrp information on switch ESRP_LAB_5.

*Q: Which is the master esrp switch for VLAN **blue**?*

Master: _____

Slave: _____

8) Display the EDP information for switch ESRP_LAB_5.

Q: How many systems are displayed?

_____

9) From your switch console, ping the **blue** interface of ESRP_LAB_1, ESRP_LAB_3, ESRP_LAB_4, and ESRP_LAB_6.

Q: Which, if any, pings are successful?

_____

10) If ESRP_LAB_5 is the Master switch noted in (7) above, turn the switch off and proceed to the end of step (12).

11) If ESRP_LAB_5 was the Slave switch noted in (7) above, wait about 10 seconds and then display the esrp information on switch ESRP_LAB_5.

*Q: Which is the master esrp switch for VLAN **blue**?*

_____

12) From your switch console, ping the **blue** interface of ESRP_LAB_1, ESRP_LAB_3, ESRP_LAB_4, and ESRP_LAB_6 again.

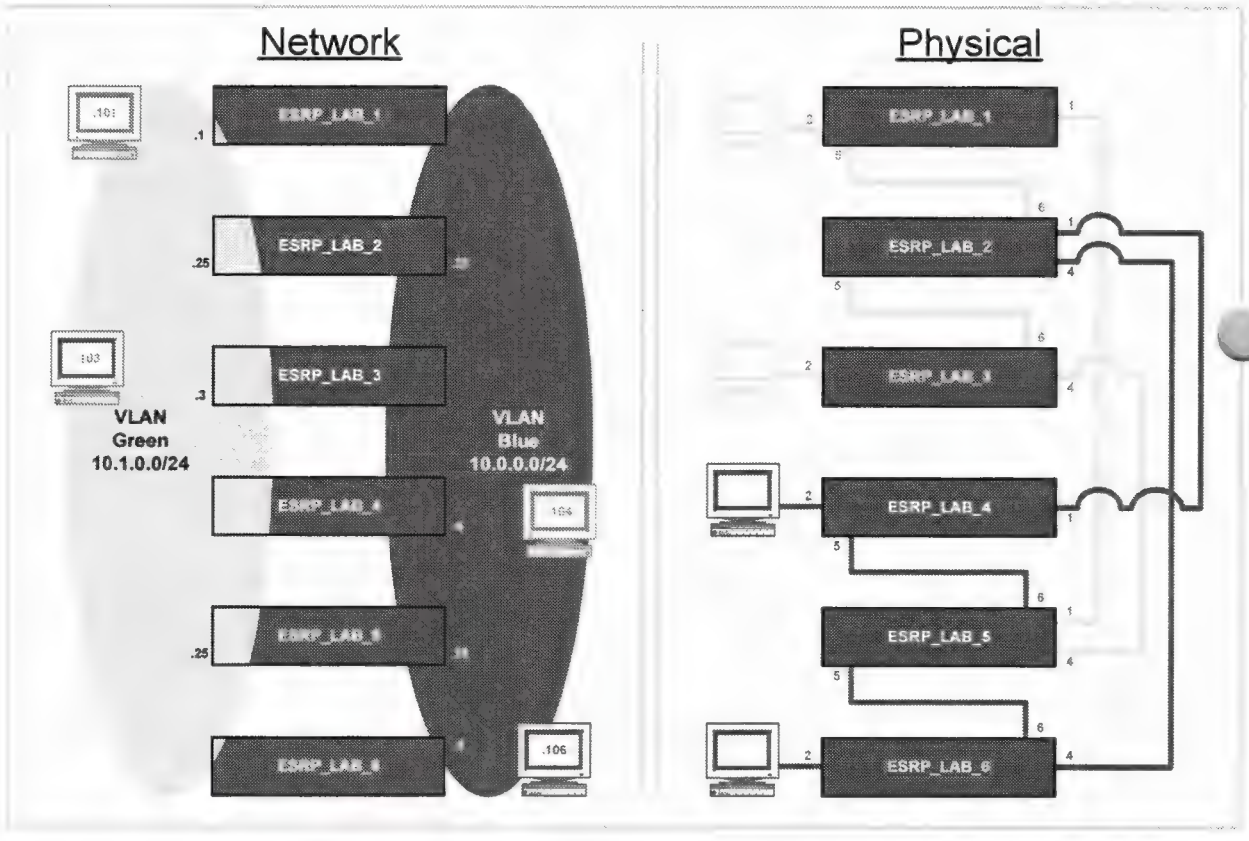
Q: Which, if any, pings are successful?

_____

Lab19 – ESRP Configuration

Wait for the team configuring the switch previously elected as Master to boot their switch before continuing.

Refer to the network diagram 1b below



13) Delete ports 1 and 4 from VLAN **blue**.

14) Create the VLAN **green,** give it an IP address in the 10.1.0.0/24 network, and assign ports 1 and 4.

15) Enable ESRP for the new VLAN **green**.

Before proceeding, confirm that the teams on ESRP_LAB_1 and ESRP_LAB_3 have completed step (15)

16) Display the esrp information on switch ESRP_LAB_5.

*Q: Which is the master esrp switch for VLAN **blue** and **green**?*

Master: _____

Before proceeding, confirm that the teams on ESRP_LAB_1 and ESRP_LAB_3 have completed step (16) and ESRP_LAB_4 and and ESRP_LAB_6 have completed step (14)

Lab19 – ESRP Configuration

SW5

17) If ESRP_LAB_5 was the Slave switch noted in (11) above, change the esrp priority for VLAN **blue** to 10 using the CLI command - **configure vlan <vlan_name> esrp priority <priority_value>.**

18) Display the esrp information for switch ESRP_LAB_5 and note which of the two switches is the ESRP master switch for the VLAN **blue**, which is the ESRP master switch for the VLAN **green**, and which switches are flagged as slave.

BLUE Master: _____ **BLUE** Slave: _____

GREEN Master: _____ **GREEN** Slave: _____

19) From the console, ping the **green** interface on ESRP_LAB_1 and ESRP_LAB_3.

Q: Which, if any, pings are successful?

_____

20) From the console, ping the **blue** interface on ESRP_LAB_4 and ESRP_LAB_6.

Q: Which, if any, pings are successful?

_____

This completes Lab19 – ESRP Configuration Lab – Switch 5

Lab19 – ESRP Configuration

SW6

1) Clear the switch of all old configuration information. Remove all cables connected from previous labs.

2) Name the switch according to the following template: ESRP_LAB_<*switch number*>

3) Delete all ports from the VLAN **default**.

4) Create the VLAN **blue,** give it an IP address in the 10.0.0.0/24 network, and assign ports 2, 4 and 6.

5) Using CAT5 cross-over patch cables, connect the following:
port 6 on ESRP_LAB_6 to port 5 on ESRP_LAB_5
port 4 on ESRP_LAB_6 to port 4 on ESRP_LAB_2
the laptop to port 2 on ESRP_LAB_6

Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (7)

6) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 and note which of the two switches is the ESRP master switch for the VLAN **blue**, and which is the slave switch.

Master: _____

Slave: _____

7) Display the EDP information for switch ESRP_LAB_6.

Q: How many systems are displayed?

_____

8) From your switch console, ping the **blue** interface of ESRP_LAB_1, ESRP_LAB_3, and ESRP_LAB_4.

Q: Which, if any, pings are successful?

_____

9) Display the ARP table on switch ESRP_LAB_6 from the switch console and note the MAC address for each of the interface addresses pinged in (8).

10) Display the forwarding database on ESRP_LAB_6.

Q: Which port is associated with the MAC addresses recorded in (9)?

_____

Wait for the team configuring the switch configured as Master (determined in step (6)) to turn off their switch before continuing.

11) Flush the ARP table and forwarding database on switch ESRP_LAB_6.

_____

Lab19 – ESRP Configuration

12) Once again, ping the **blue** interface of ESRP_LAB_1, ESRP_LAB_3, and ESRP_LAB_4 from the switch console.

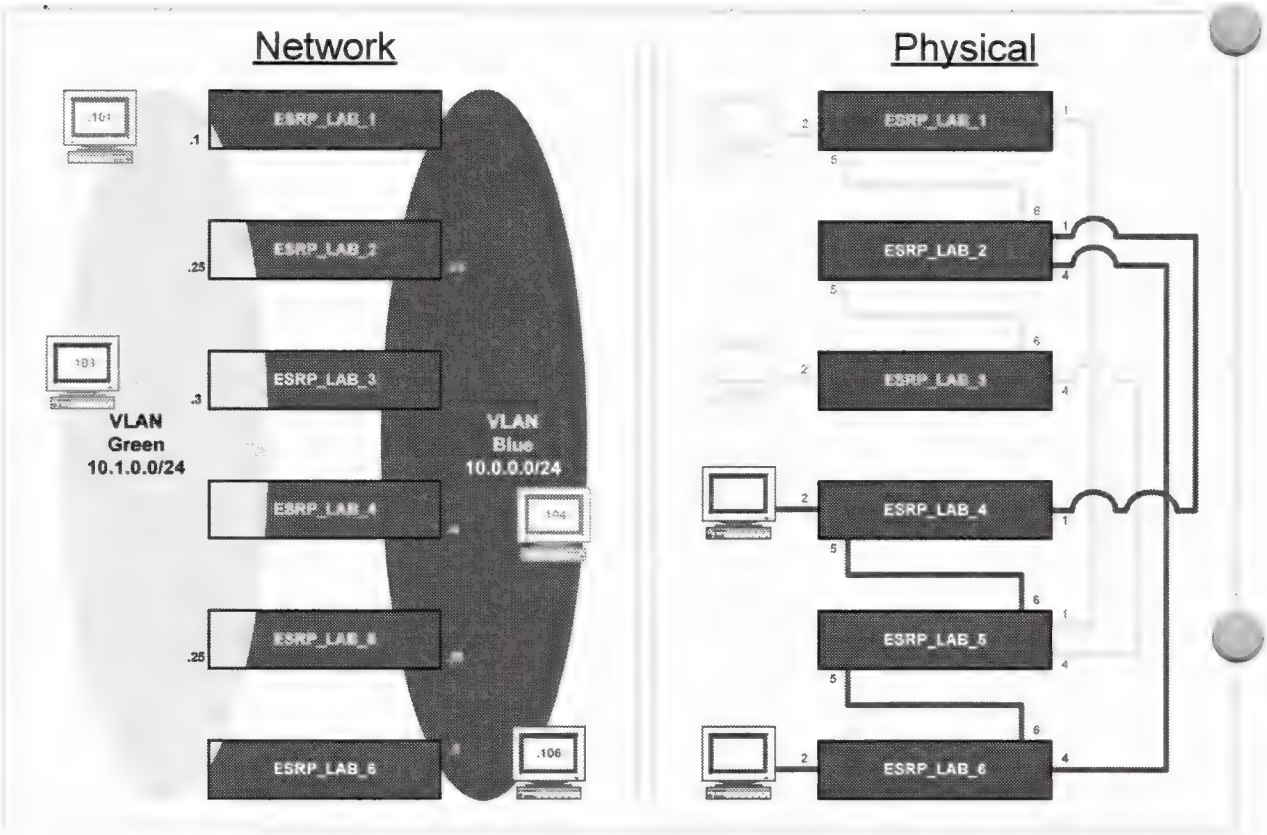
Q: Which, if any, pings are successful?

13) Now display the forwarding database on ESRP_LAB_6.

Q: Which port is associated with the MAC addresses recorded in (9)?

Wait for the team configuring the switch previously elected as Master to boot their switch before continuing.

Refer to the network diagram 1b below



Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (16)

14) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 and note which of the two switches is the ESRP master switch for both of the VLANs **blue** and **green**.

Master: _____

Lab19 – ESRP Configuration

SW6

Before proceeding, confirm that the teams on ESRP_LAB_2 and ESRP_LAB_5 have completed step (17)

15) Consult with the teams configuring ESRP_LAB_2 and ESRP_LAB_5 once more and note which of the two switches is the ESRP master switch for the VLAN **blue**, which is the ESRP master switch for the VLAN **green**, and which switches are flagged as slave.

BLUE Master: _____ **BLUE** Slave: _____

GREEN Master: _____ **GREEN** Slave: _____

16) From the console, ping the **blue** interface on ESRP_LAB_4.

17) Display the forwarding database on ESRP_LAB_6.

Q: Which port is associated with the MAC address of ESRP_LAB_4?

18) Disconnect the appropriate cable connected to the **blue** master switch noted in (15) above.

19) Once more, ping the **blue** interface on ESRP_LAB_4 from the console,.

20) Display the forwarding database on ESRP_LAB_6.

Q: Which port is associated with the MAC address of ESRP_LAB_6?

This completes Lab19 – ESRP Configuration Lab – Switch 6

Lab 20 – QoS Configuration

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Configure a network of switches to demonstrate the QoS feature
2. Configure the network for QoS using the CLI command – **config vlan qosprofile <qosprofile>**
3. Change the QoSprofile and observe the effects on the network's performance.

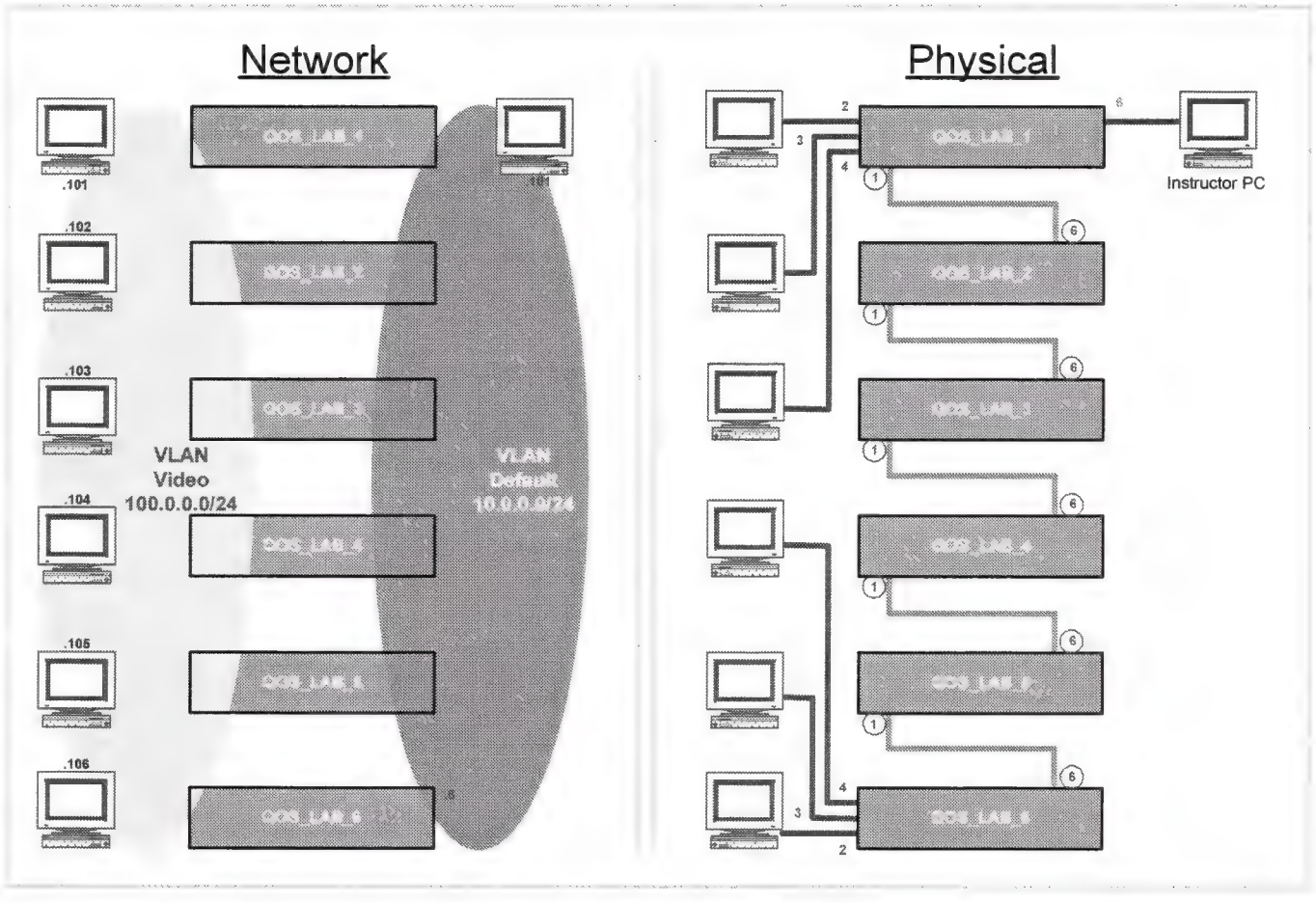
MATERIALS REQUIRED:

1. Extreme LAN switch (I-based desktop like Summit1i or equivalent) and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Cross-over and straight-thru cables as required + console cable
4. Spoiler application (**wsttcp.exe**) from Instructor PC and the Video movie application in each PC/laptop – **corpvideo.mov**

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide version 6.1+ (if available)

PROCEDURES:



Lab 20 – QoS Configuration

SW1

NOTE: There will be 2 VLANs that are active in the configured network. Create VLAN video. You will configure an IP address on the PC/Laptop, reboot and login and then access the file ***corpvideo.mov*** *and set it to continuous play. The instructor PC via tagging will be generating the traffic.*

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: QOS_LAB_*<switch number>*

3) Delete ports 2, 3, and 4 from VLAN **default** and assign an interface of 10.0.0.1/24

4) Create the VLAN **video**, give it an explicit tag of **10**, and assign port 1 tagged, and ports 2, 3, and 4, untagged.

5) Reduce the port speed on port 1 to 10Mb from the default 100Mb

6) Using a cross-over cable, connect port 1 on QOS_LAB_1 to port 6 on QOS_LAB_2

7) The instructor's laptop from QOS_LAB_1 will be the 'network spoiler', transmitting a steady UDP stream of data across all six switches to an interface on QOS_LAB_6.

   Configure the QOS_LAB_1 laptop with the following parameters:

   IP Address = 100.0.0.101
   IP Mask = 255.255.255.0
   Gateway = <none>

8) Using a regular ethernet cable, connect the laptop to port 2 on the switch. Connect the laptop from station 2 to port 3 on the switch and connect the laptop from station 3 to port 4 on the switch.

9) When all of the lab teams have their switches and laptops fully configured, open the **c:\corpvideo.mov** file on the laptop named **student04.**

   Observe the performance of the video stream in your Player. The video should be running clear and without interruption.

10) Continue to observe your Player's performance as the instructor connects his/her PC/laptop to port 6 of QOS_LAB_1 and launches the network 'spoiler' application.

    Q: Has there been a change in performance since launching the 'spoiler' application?

    _____

11) Coordinating with the teams on all six switches, change the QoS profile for the VLAN **video** to QP2.

    Q: Is there a change in the video performance?

    _____

_____

Lab 20 – QoS Configuration

SW1

12) Again, coordinating with the teams on all six switches, change the QoS profile for the VLAN **default** to QP3.

Q: Is there a change in the video performance?

_____

13) For the last step, coordinate with the other teams and change the minimum bandwidth reservation for QP2 to 60%.

Q: Is there a change in the video performance?

_____

This completes the Lab20 – QoS Configuration Lab – for Switch 1.

Lab 20 – QoS Configuration

SW2

NOTE:
There will be 2 VLANs that are active in the configured network. Create VLAN video. You will configure an IP address on the PC/Laptop, reboot and login and then access the file corpvideo.mov and set it to continuous play. The instructor PC via tagging will be generating the traffic.

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: QOS_LAB_*<switch number>*

3) Create the VLAN **video**, give it an explicit tag of **10**, and assign ports 1 and 6 tagged.

4) Reduce the port speed on ports 1 and 6 to 10Mb from the default 100Mb.

5) Using a cross-over cable, connect port 6 on QOS_LAB_2 to port 1 on QOS_LAB_1 and port 1 on QOS_LAB_2 to port 6 on QOS_LAB_3.

6) The laptop from QOS_LAB_2 will act as both the client and the server for the video stream provided by **corpvideo.mov** file.

   Configure the QOS_LAB_2 laptop with the following parameters:

   IP Address = 100.0.0.102
   IP Mask = 255.255.255.0
   Gateway = <none>

7) Using a regular ethernet cable, connect the laptop to port 3 of QOS_LAB_1.

8) When all of the lab teams have their switches and laptops fully configured, open the **c:\corpvideo.mov** file on the laptop named **student05.**

   Observe the performance of the video stream in your Player. The video should be running clear and without interruption.

9) Continue to observe your Player's performance as the instructor connects his/her PC/laptop to port 6 of QOS_LAB_1 and launches the network 'spoiler' application.

   Q: Has there been a change in performance since launching the 'spoiler' application?

   _____

10) Observe the network performance and monitor the coordination happening between Switch 1 and Switch 6. The qosprofile will be configured for the VLAN **video** and **default** for these switches.

This completes the Lab20 – QoS Configuration Lab – for Switch 2.

_____

Lab 20 – QoS Configuration

SW3

NOTE:
There will be 2 VLANs that are active in the configured network. Create VLAN video. You will configure an IP address on the PC/Laptop, reboot and login and then access the file corpvideo.mov and set it to continuous play. The instructor PC via tagging will be generating the traffic.

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: QOS_LAB_<*switch number*>

3) Create the VLAN **video**, give it an explicit tag of **10**, and assign ports 1 and 6 tagged.

4) Reduce the port speed on ports 1 and 6 to 10Mb from the default 100Mb.

5) Using a cross-over cable, connect port 6 on QOS_LAB_3 to port 1 on QOS_LAB_2 and port 1 on QOS_LAB_3 to port 6 on QOS_LAB_4.

6) The laptop from QOS_LAB_3 will act as both the client and the server for the video stream provided by **corpvideo.mov** file.

   Configure the QOS_LAB_3 laptop with the following parameters:

   IP Address = 100.0.0.103
   IP Mask = 255.255.255.0
   Gateway = <none>

7) Using a regular ethernet cable, connect the laptop to port 4 of QOS_LAB_1.

8) When all of the lab teams have their switches and laptops fully configured, open the **c:\corpvideo.mov** file on the laptop named **student06.**

   Observe the performance of the video stream in your Player. The video should be running clear and without interruption.

9) Continue to observe your Player's performance as the instructor connects his/her PC/laptop to port 6 of QOS_LAB_1 and launches the network 'spoiler' application.

   Q: Has there been a change in performance since launching the 'spoiler' application?

   _____

10) Observe the network performance and monitor the coordination happening between Switch 1 and Switch 6. The qosprofile will be configured for the VLAN **video** and **default** for these switches.

This completes the Lab20 – QoS Configuration Lab – for Switch 3.

_____

Lab 20 – QoS Configuration

SW4

NOTE:
There will be 2 VLANs that are active in the configured network. Create VLAN video. You will configure an IP address on the PC/Laptop, reboot and login and then access the file corpvideo.mov and set it to continuous play. The instructor PC via tagging will be generating the traffic.

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: QOS_LAB_<*switch number*>

3) Create the VLAN **video**, give it an explicit tag of **10**, and assign ports 1 and 6 tagged.

4) Reduce the port speed on ports 1 and 6 to 10Mb from the default 100Mb.

5) Using a cross-over cable, connect port 6 on QOS_LAB_4 to port 1 on QOS_LAB_3 and port 1 on QOS_LAB_4 to port 6 on QOS_LAB_5.

6) The laptop from QOS_LAB_4 will act as both the client and the server for the video stream provided by **corpvideo.mov** file.

   Configure the QOS_LAB_4 laptop with the following parameters:

   IP Address = 100.0.0.104
   IP Mask = 255.255.255.0
   Gateway = <none>

7) Using a regular ethernet cable, connect the laptop to port 4 of QOS_LAB_6.

8) When all of the lab teams have their switches and laptops fully configured, open the **c:\corpvideo.mov** file on the laptop named **student06.**

   Observe the performance of the video stream in your Player. The video should be running clear and without interruption.

9) Continue to observe your Player's performance as the instructor connects his/her PC/laptop to port 6 of QOS_LAB_1 and launches the network 'spoiler' application.

   Q: Has there been a change in performance since launching the 'spoiler' application?

   _____

10) Observe the network performance and monitor the coordination happening between Switch 1 and Switch 6. The qosprofile will be configured for the VLAN **video** and **default** for these switches.

This completes the Lab20 – QoS Configuration Lab – for Switch 4.

_____

Lab 20– QoS Configuration

SW5

NOTE:
There will be 2 VLANs that are active in the configured network. Create VLAN video. You will configure an IP address on the PC/Laptop, reboot and login and then access the file corpvideo.mov and set it to continuous play. The instructor PC via tagging will be generating the traffic.

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: QOS_LAB_*<switch number>*

3) Create the VLAN **video**, give it an explicit tag of **10**, and assign ports 1 and 6 tagged.

4) Reduce the port speed on ports 1 and 6 to 10Mb from the default 100Mb.

5) Using cross-over cables, connect port 6 on QOS_LAB_5 to port 1 on QOS_LAB_4 and port 1 on QOS_LAB_5 to port 6 on QOS_LAB_6.

6) The laptop from QOS_LAB_5 will act as both the client and the server for the video stream provided by **corpvideo.mov** file.

   Configure the QOS_LAB_5 laptop with the following parameters:

   IP Address = 100.0.0.105
   IP Mask = 255.255.255.0
   Gateway = <none>

7) Using a regular ethernet cable, connect the laptop to port 3 of QOS_LAB_6.

8) When all of the lab teams have their switches and laptops fully configured, open the **c:\corpvideo.mov** file on the laptop named **student02.**

   Observe the performance of the video stream in your Player. The video should be running clear and without interruption.

9) Continue to observe your Player's performance as the instructor connects his/her PC/laptop to port 6 of QOS_LAB_1 and launches the network 'spoiler' application.

   Q: Has there been a change in performance since launching the 'spoiler' application?

   _____

10) Observe the network performance and monitor the coordination happening between Switch 1 and Switch 6. The qosprofile will be configured for the VLAN **video** and **default** for these switches.

This completes the Lab20 – QoS Configuration Lab – for Switch 5.

_____

Lab 20– QoS Configuration

SW6

NOTE:
There will be 2 VLANs that are active in the configured network. Create VLAN video. You will configure an IP address on the PC/Laptop, reboot and login and then access the file corpvideo.mov and set it to continuous play. The instructor PC via tagging will be generating the traffic.

1) Clear the switch of all old configuration information.

2) Name the switch according to the following template: QOS_LAB_<*switch number*>

3) Delete ports 2, 3, and 4 from VLAN **default** and assign it an interface of 10.0.0.6/24

4) Create the VLAN **video**, give it an explicit tag of **10**, and assign port 6 tagged, and ports 2, 3, and 4, untagged.

5) Reduce the port speed on port 6 to 10Mb from the default 100Mb

6) Using a cross-over cable, connect port 1 on QOS_LAB_5 to port 6 on QOS_LAB_6

7) The laptop from QOS_LAB_6 will act as both the client and the server for the video stream provided by **corpvideo.mov** file.

   Configure the QOS_LAB_6 laptop with the following parameters:

   IP Address = 100.0.0.106
   IP Mask = 255.255.255.0
   Gateway = <none>

8) Using a regular ethernet cable, connect the laptop to port 2 on the switch. Connect the laptop from station 5 to port 3 on the switch and connect the laptop from station 4 to port 4 on the switch.

9) When all of the lab teams have their switches and laptops fully configured, open the **c:\corpvideo.mov** file on the laptop named **student03.**

   Observe the performance of the video stream in your Player. The video should be running clear and without interruption.

10) Continue to observe your Player's performance as the instructor connects his/her PC/laptop to port 6 of QOS_LAB_1 and launches the network 'spoiler' application.

    Q: Has there been a change in performance since launching the 'spoiler' application?

    _____

Lab 20– QoS Configuration

SW6

11) Coordinating with the teams on all six switches, change the QoS profile for the VLAN **video** to QP2.

Q: Is there a change in the video performance?

_____

12) Again, coordinating with the teams on all six switches, change the QoS profile for the VLAN **default** to QP3.

Q: Is there a change in the video performance?

_____

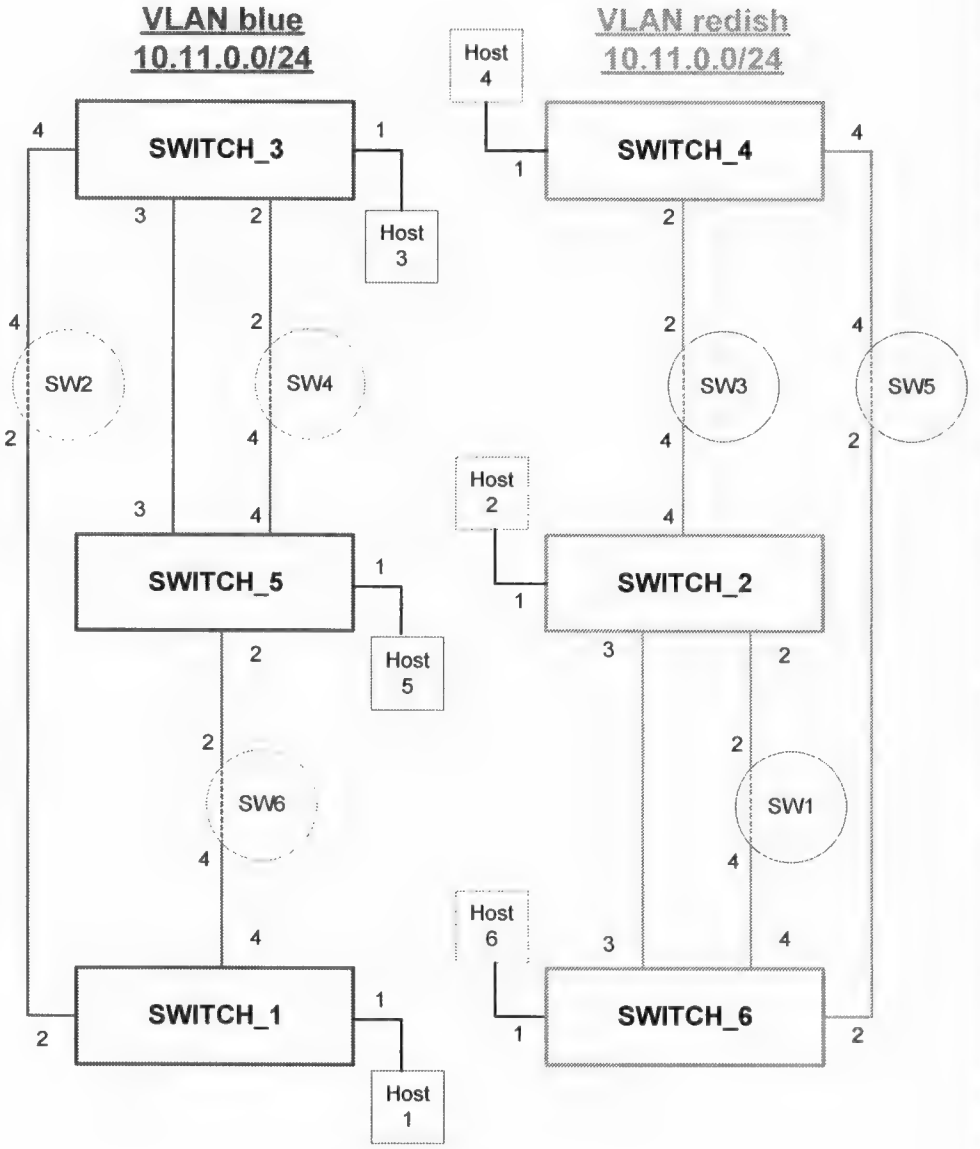
13) For the last step, coordinate with the other teams and change the minimum bandwidth reservation for QP2 to 60%.

Q: Is there a change in the video performance?

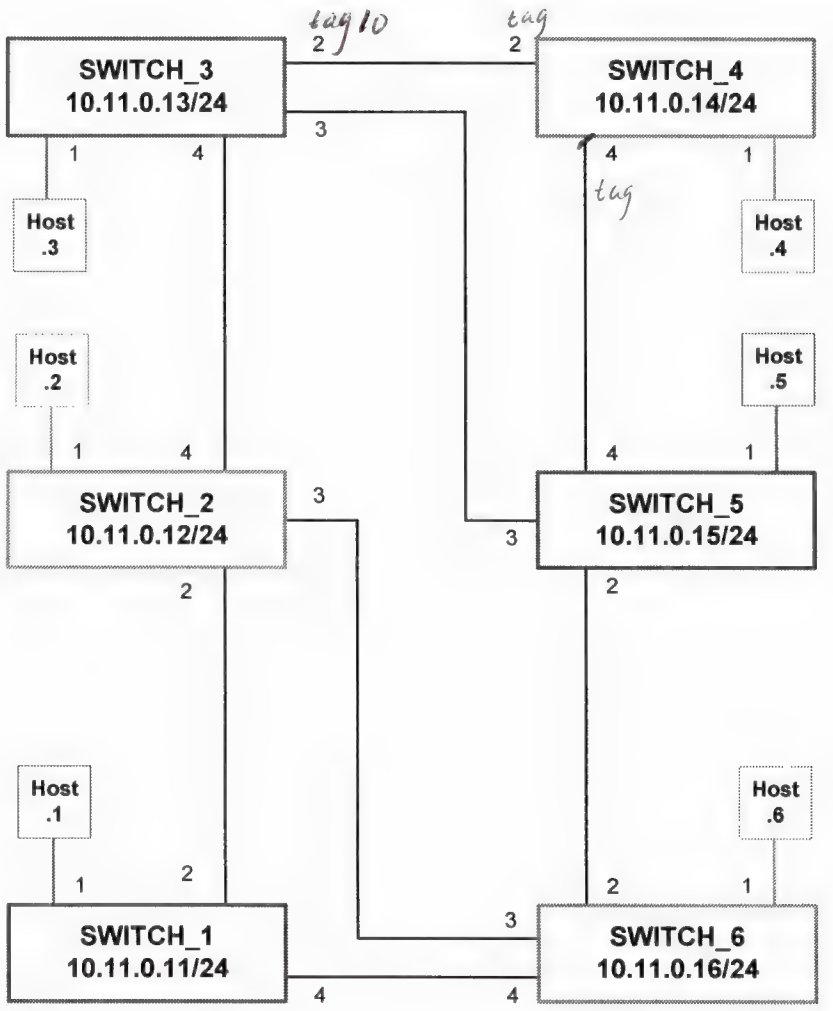
_____

This completes the Lab20 – QoS Configuration Lab – for Switch 6.

Challenge 1 - L2 Network Challenge



red 10
Blue 20.



C1 – L2 Network Challenge

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Determine the configuration errors on a network of switches setup by the instructor
2. Troubleshoot and correct the network of switches based on all the knowledge acquired in this 3-days of technical training.
3. Fully appreciate the value of being able to setup, configure, verify and troubleshoot Extreme switches using CLI Configuration and Management in a Layer 2 Environment.

The **goal** of the challenge exercise is to **troubleshoot and restore** the network to the state as depicted on the Lab 21 – Network Challenge diagram. This simulates a network situation where you have many users on the network. Therefore… ***DO NOT*** **UNCONFIGURE THE SWITCHES AND TRY TO RE-BUILD THE LAB SCENARIO FROM SCRATCH.**

MATERIALS REQUIRED:

1. Summit1i LAN switch and power cord or equivalent
2. PC/Laptop + NIC plus terminal emulation software
3. Colored Network Topology Diagram – from Instructor (also projected on the screen)
4. Network cables as required

REFERENCES:

1. Lab procedures from the Training Manual
2. ExtremeWare Software User Guide rev 6.1+(if available)

PROCEDURES:

1. On your mark…
2. Get Set…
3. Go!
   ** Helpful Tip: Keep a record of ALL changes made to the switch so that you can compare your findings with the solutions the instructor will provide

You will be instructed as to when to start the Challenge Exercise.

The allocated time to put the network back in shape is approximately 60-90 minutes. Good Luck!

C2 – Layer 3 Network Challenge Exercise

OBJECTIVES:

Upon successful completion of this Lab Exercise, the student will be able to:

1. Determine the configuration errors on a network of switches setup by the instructor
2. Troubleshoot and correct the network of switches based on all the knowledge he acquired in this 5-days of technical training.
3. Fully appreciate the value of being able to setup, configure, verify and troubleshoot Extreme switches for Unicast Routing and Layer 3 environments.

MATERIALS REQUIRED:

1. Summit LAN switch and power cord
2. PC/Laptop + NIC plus terminal emulation software
3. Colored Network Topology Diagram – from Instructor (also projected on the screen)
4. Patch cable, fiber-optic cross-over cable.

REFERENCES:

1. Lab procedures from the Student Guide
2. Summit Switch User Guide (if available)

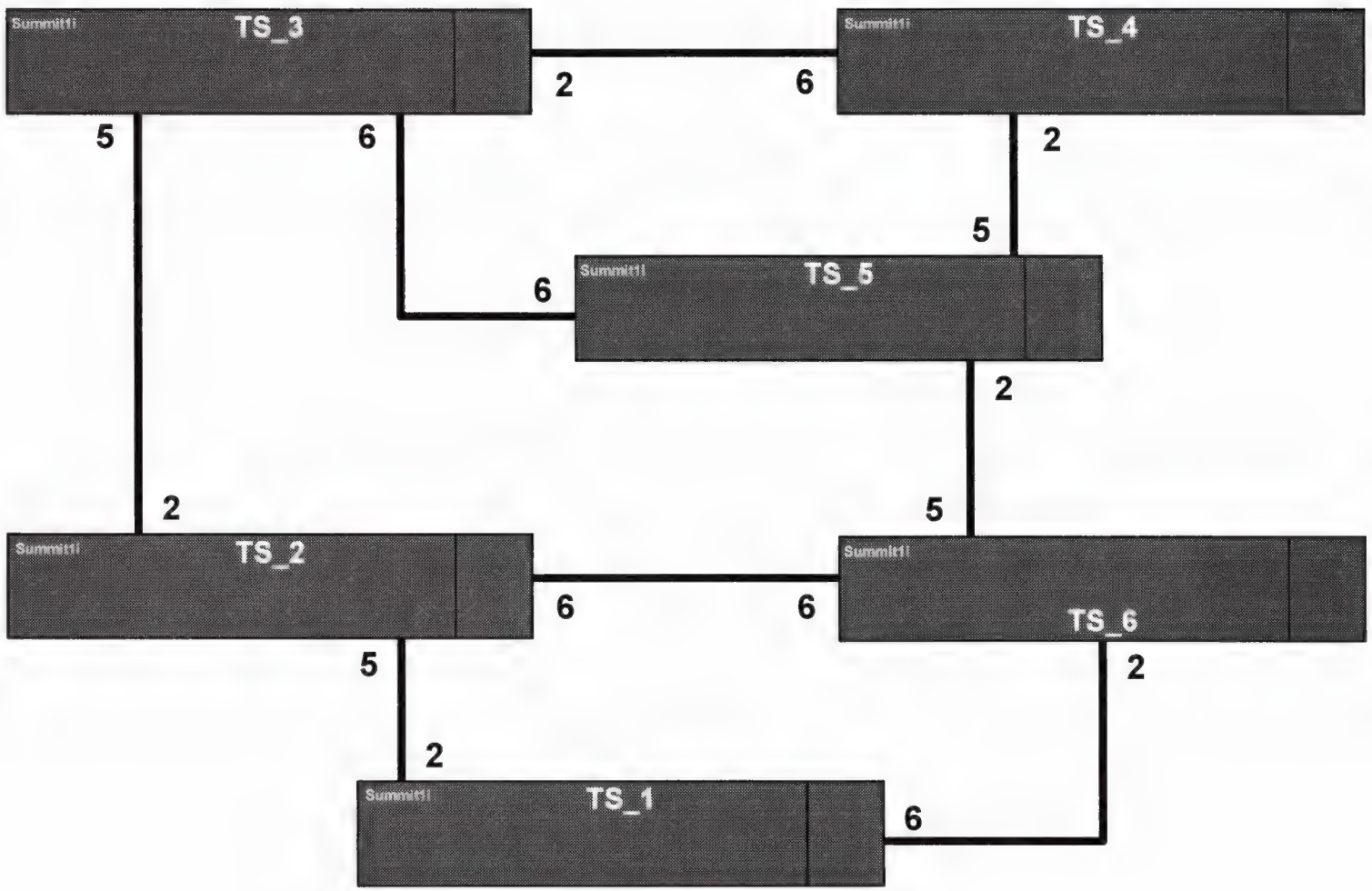
PROCEDURES:

1. On your mark…
2. Get Set…
3. Go!

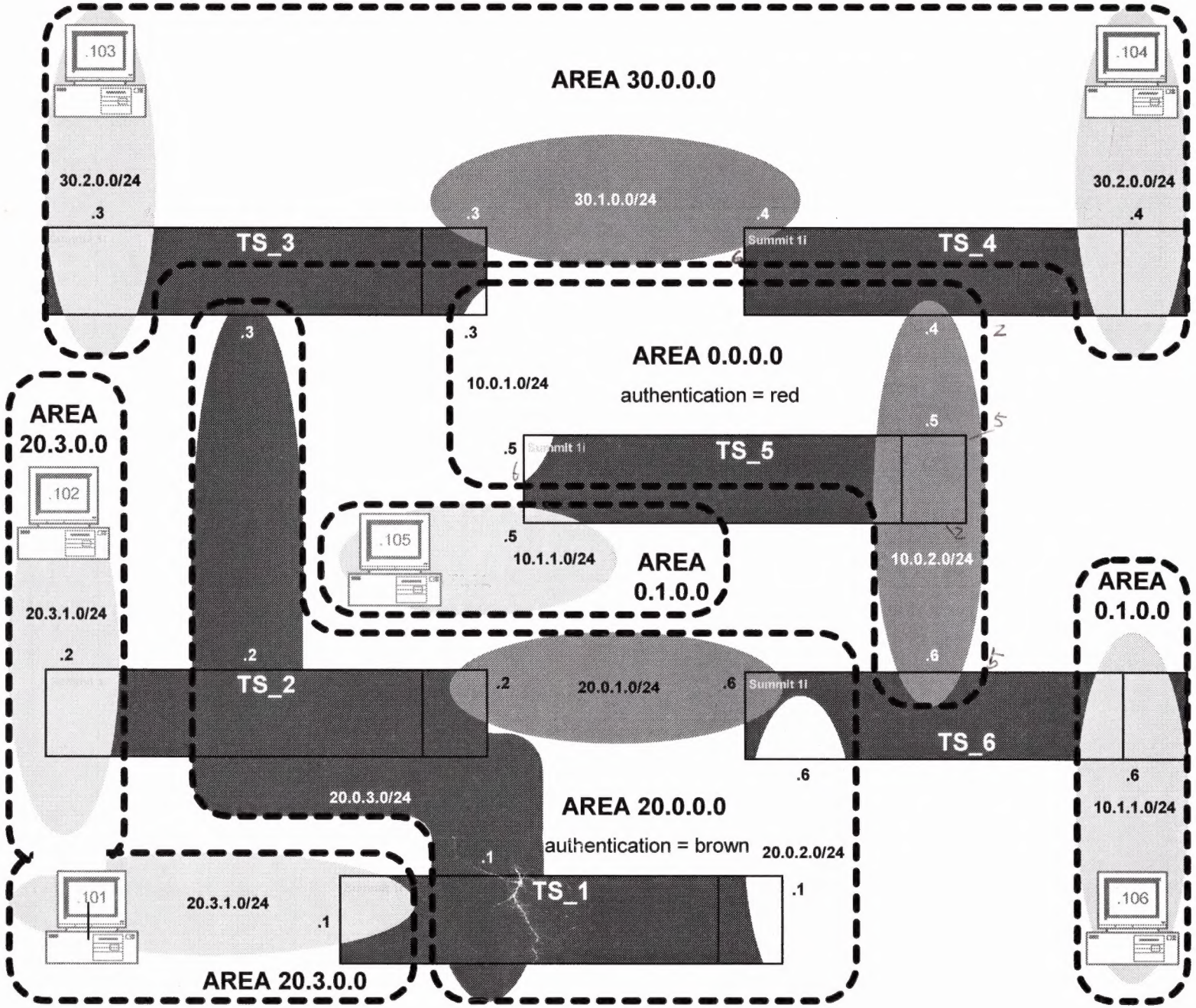
The students will be instructed as to when to start their challenge exercise.

The allocated time to put the network back in shape is approximately 60-90 minutes. Good Luck!

Challenge 2 - L3 Network Challenge
Physical Network



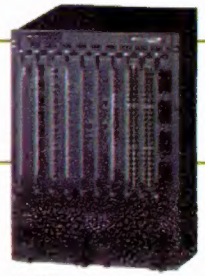
Challenge 2 - L3 Network Challenge



MOI
Terve
Moido

EXTREME NETWORKS®

products AT A GLANCE



BlackDiamond 6808

BLACKDIAMOND® 6800 SERIES

Ideally suited for network core and data centers where high density and availability are crucial.

- Fully redundant, load-sharing, hot-swappable power supplies and modules
- MPLS module enables Layer 2/Layer 3 transparent LAN services
- WDMi module optically multiplexes 8 full-duplex gigabit channels into a single-mode fiber pair for medium reach MAN and campus applications
- Packet-over-SONET module provides connectivity to SONET/SDH legacy infrastructure
- ARM module allows differential billing based on the destination of IP unicast traffic

Alpine 3808

ALPINE™ 3800 SERIES

Ideal for use throughout the network where flexibility, price/performance ratio and legacy WAN connectivity are the primary objectives.

- Fully redundant, load-sharing, hot-swappable power supplies and modules
- VDSL module extends Ethernet into MTU and campus networks over voice-grade wiring with a range of 3000 ft., when fiber or Category 5(CAT5) cabling is not available
- T1, E1 and DS3 modules deliver Ethernet in the First Mile
- WDMi module optically multiplexes 4 full-duplex gigabit channels into a single-mode fiber pair for medium reach MAN and campus applications

SUMMIT48i™

The ideal advanced 10/100 Mbps aggregation switching solution for deploying sophisticated features and Layer 3 intelligence at the edge of the network.

Summit7i

SUMMIT1i/5i/7i™

Stackable, fixed-configuration switches, ideal for mid-tier aggregation applications in small to medium networks when cost and space constraints are of utmost importance.

"i" SERIES CHIPSET FEATURES

"i" series chipset features found in all BlackDiamond, Alpine and Summit "i" switches

- Wire-speed IP/IPX routing using RIP v1/v2, OSPF, BGP4, PIM and DVMRP
- Policy-Based Quality of Service (PB QoS) at wire speed to allocate bandwidth and prioritize traffic
- Access Control Lists (ACLs) for increased security and traffic control
- Ethernet Automatic Protection Switching (EAPS) delivers sub-second link failover for ring-based Ethernet topology
- Network Login provides an Ethernet post-based access control mechanism using RADIUS

extreme networks

www.extremenetworks.com

Summit24e2

SUMMIT24e™ SERIES

Ideal for delivering Layer 2 and/or Layer 3 switching to the edge of the network at a cost-effective price point to satisfy constrained budgets.

Summit48

SUMMIT24/48™

Integrating seamlessly into the access layer of the network these switches provide 10/100 Mbps aggregation delivering high port density, wire-speed performance and low cost of ownership.

SUMMITPx1™

Award-winning Layer 4-7 application load balancing delivering 10x performance gain with 1 million Layer 7 sessions and 3 million Layer 4 sessions simultaneously at wire speed. Software-based networking functions performed entirely in hardware.

INFRASTRUCTURE & SERVICES MANAGEMENT (ISM)

Extreme's next-generation network management software family simplifies and automates Layer 2-7 application infrastructures allowing for an overall improved end user experience.

- EPICenter™ – an integrated application suite that simplifies configuration, troubleshooting, and status monitoring of IP-based networks
- EPICenter Policy Manager – provides layer-independent policy enforcement for Layers 1-4
- ServiceWatch® – delivers powerful, Layer 4-7 monitoring and management for mission-critical network services such as e-mail, e-commerce, and file transfer

products AT A GLANCE

features	BLACKDIAMOND 6816	BLACKDIAMOND 6808	ALPINE 3808	ALPINE 3804	ALPINE 3802	SUMMIT1i	SUMMIT5i	SUMMIT7i	SUMMIT48i	SUMMIT24	SUMMIT48	SUMMIT24e3	SUMMIT24e2	SUMMITPx1
GIGABIT ETHERNET PORTS	up to 192	up to 96	up to 32	up to 16	up to 8	8 Fixed (6+2)	16 Fixed (12+4)	32 Fixed (28+4)	2 Fixed	1 Fixed	2 Fixed	2 Fixed	2 Fixed	1 Fixed
AUTO-NEGOTIATIONG 10/100BASE-TX PORTS	up to 1440	up to 384	up to 256	up to 128	up to 64	100/1000 Mbps only	100/1000 Mbps only	100/1000 Mbps only	48 Fixed	24 Fixed	48 Fixed	24 Fixed	24 Fixed	N/A
FORM FACTOR/FOOTPRINT	Chassis/35RU	Chassis/15RU	Chassis/12RU	Chassis/6RU	Chassis/4RU	Stackable/2RU	Stackable/2RU	Stackable/4RU	Stackable/2RU	Stackable/2RU	Stackable/2RU	Stackable/1RU	Stackable/1RU	1RU
SWITCH FABRIC BANDWIDTH	256 Gbps	128 Gbps	64 Gbps	32 Gbps	16 Gbps	17.5 Gbps	32 Gbps	64 Gbps	17.5 Gbps	8.5 Gbps	17.5 Gbps	8.8 Gbps	8.8 Gbps	2 Gbps
PACKETS-PER-SECOND FORWARDING RATE	192 Million	96 Million	48 Million	24 Million	12 Million	12 Million	23.8 Million	48 Million	10.1 Million	5.1 Million	10.1 Million	6.6 Million	6.6 Million	1.5 Million
POLICY-BASED QUALITY OF SERVICE (QoS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
WIRE-SPEED LAYER 2/LAYER 3 SWITCHING	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	L2	L4-L7
INTEGRATED SERVER LOAD BALANCING	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes
TRANSPARENT WEB CACHE REDIRECTION	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
NETWORK LOGIN AND EAPS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
ACCESS CONTROL LISTS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
LINK AGGREGATION	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
REDUNDANT POWER	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
SWITCH MANAGEMENT CAPABILITIES	SNMP, Web, CLI, 4 RMON groups	SNMP, Web, CLI, 4 RMON groups	SNMP, Web, CLI, 4 RMON groups	SNMP, Web, CLI, 4 RMON groups	SNMP, Web, CLI, 4 RMON groups	CLI, 4 RMON groups	SNMP, Web, CLI, 4 RMON groups	SNMP, Web, CLI, 4 RMON groups	SNMP, Web, CLI, 4 RMON groups	SNMP, Web, CLI, 4 RMON groups	SNMP, Web, CLI, 4 RMON groups	SNMP, Web, CLI, 4 RMON groups	SNMP, Web, CLI, 4 RMON groups	SNMP, CLI
NETWORK MANAGEMENT	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BGP4, DVMRP, OSPF, PIM, RIP v1/v2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	RIP v1/v2, OSPF, PIM, DVMRP	RIP v1/v2, OSPF, PIM, DVMRP	RIP v1/v2	N/A	N/A
SPANNING TREE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A

extreme networks

3585 Monroe Street Santa Clara, CA 95051-1450 Phone 408.579.2800 Fax 408.579.3000
Email info@extremenetworks.com Web www.extremenetworks.com

© 2001 Extreme Networks, Inc. All rights reserved. Extreme Networks, BlackDiamond, Summit, ExtremeWare, ServiceWatch, Extreme Ethernet Everywhere, Ethernet Everywhere, Extreme Velocity, Extreme Turbodrive and the color purple are registered trademarks of Extreme Networks, Inc. in certain jurisdictions. Alpine, ExtremeWare Vista, Extreme Standby Router Protocol, ESRP, Summit1i, Summit4, Summit4/FX, Summit5i, Summit7i, Summit24, Summit24e2, Summit24e3, Summit48, Summit48i, SummitLink, SummitGbX, SummitRPS, SummitPx1, PxSilicon, EPICenter, vMAN, the BlackDiamond logo, the Alpine logo and the Extreme Networks logo are trademarks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. ExtremeWorks, the Extreme Turbodrive logo and the Go Purple-Extreme Solution Partners logo are service marks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. All other registered trademarks, trademarks and service marks are property of their respective owners. Specifications are subject to change without notice.

L-BR-PAG-111